

تعرف على تقنية الحوسبة السحابية Cloud Computing



- توفير مبالغ ضخمة
- توفير خدمات مختلفة
- توفير معدات وتقنيات شبكية

نتائج الاستفتاء

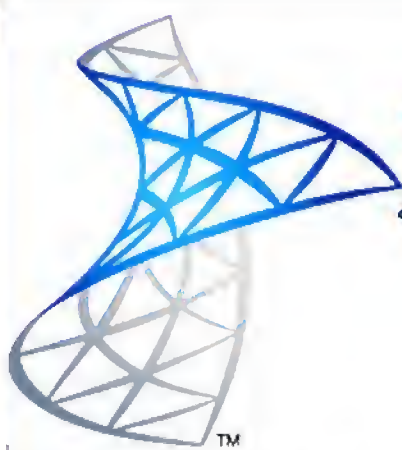
هل أنت من مؤيدي الباس فور شور؟

• نعم

76%

• لا

24%



Microsoft®

System Center

تعرف على عائلة سيرفرات مركز
نظام مايكروسوفت

تقرأون في هذا العدد

ماهي الـ RFC وماذا تعني؟

RFC

Request For Comments

مقارنة بين سويتشات الطبقة
الثانية والثالثة وMLS

ما هو الـ RADIUS Server

خمس أشياء يجب أن تعرفها
عن سويتشات سيسكو

أهم الكتب والمراجع الخاصة
بدراسة شهادات جونيبر

والعديد من المواضيع
الجديدة والقيمة

شاهدوا أيضا أقسام

مصطلحات تقنية



عتاد ومعلومات



مشاكل وحلول



4



أفتتاحية العدد

امنية دراسه ومعجزة وظيفه

المحررون الدائمون

- الدكتور محمد التميمي

Yarra_link@yahoo.com

- المهندس أيمن النعيمي

www.networkset.net

- المهندس أحمد الشحات

warior10@hotmail.com

- المهندس عادل الحميدي

adel_husni2000@hotmail.com

- المهندس ياسر رمزي

www.yasserauda.com

المحررون الضيوف

- المهندس أحمد بخيت

www.abakhiet.info

حينما يرغب احدنا في بناء المستقبل يجد عوائق من بينها ضعف المناهج المقدمه خلال سنوات دراسته ليجد نفسه اما يدرس مالا يحب او يتخرج وهو لا يفقه ابجديات العلم الذي تمنى تعلمه وهكذا دول لاتجد في دوائرها الا موظفي الراتب اولئك الذين يتعين اغلبهم من خلال الواسطه لهذا تهرول دولنا خلفا لان تقدم الامم بجامعاتها ومناهجها التعليميه ومنه تتطور الامه في مصانعها ودوائرها وحتى اسلوب الحياه.

كذلك الحال في مناهجنا التعليميه العلميه فالطالب يدرس 12سنة تمهيدا لدخول الجامعة وهو لايعلم مالفائده من استخدام داله اللوغارتم مثلا في الحياه العمليه وهكذا يبلغ حوالي 18سنة وهو لم يختص في الاختصاص الذي يرغب بالعمل فيه بعد. ثم اربع سنوات جامعيه يقضيها في دراسه تاريخ الاختصاص فمابين المخترع الفلاني وحدث في مثل هذا اليوم قبل الف عام تضيع السنه الاولى وتتبعها ثلاث اخر يتم فيها اضافته مناهج لاعلاقه لها بصميم الاختصاص او يكون المحاضر من رعيه الديناصورات يفهم في النظريات فقط اضافته الى المنهج الدولي يتغير بمعدل مره كل نصف عام اما في جامعاتنا فالمنهج يتغير مره في احسن الاحوال كل عشره اعوام.

وتتخرج وعمره 22سنة وفي اغلب البلدان تكون هديه التخرج هي الخدمه العسكريه التي وظيفتها مسح كل ماتعملته خلال السنوات الاربعه وبعدها البحث عن وظيفه وانت بلا مؤهل فترفضك الدوائر الحكوميه المئينه بالبطاله المقتنعه وترفضك الشركات الخاصه لانها تشترط الخبره لتصل الى منتصف العشرين وانت الى الان لم تعمل شيء. مقارنة مع استراليا مثلا التخصص يبدأ من المرحلة الثانويه , لديك دراسه ثلاث سنوات تختار فيها المواد القريبه من اختصاصك وان حققت معدل ودعمت الامر بخبره تأتي من خلال العمل التطوعي المتاح يتم قبولك في الجامعة او تدعم دراستك بكورسات او دبلوم من التيف TAFE وهي مؤسسه معنيه بتقديم خدمات عمليه للطلبة بكورسات تبدأ بمدد من الشهر وتنتهي بالثلاثه سنوات وبعدها اما العمل لانك تاهلت او التقديم للجامعة وفي الغالب كثيرون يكتفون بشهاده التيف فتجد الشاب يكون عمره 20سنة وهو يمتلك الخبره الحقيقيه للعمل وطالما هنالك خبره وسوق عمل حقيقي فهناك وظائف جديده وهناك بلد ينمو ويتطور. اما عن الرواتب ففي دولنا تكون من خلال الترفيه كل اربع سنوات سواء كنت تعمل او لم تكن بحيث يصل الجميع بعد حين الى نتيجته واحده ان كنت انا وزميلي النائم بجانبك تكون الترفيه لكلينا فلماذا لا اعط في نوم عميق بدل من النجاح الذي سيفتق زملائي ومديري قبلهم ؟ مقارنة مع الدول فنظام العمل يكون من خلال عقود سنويه ان لبيت الشروط ازداد راتبك في العقد الاخر وربما الشركات الاخرى عرضت عليك عروض افضل فبالنتيجه يكون الجميع في حاله عمل فعليه تنعكس على البلاد والعباد.

وهنا نتساءل كيف للدوله ان تحقق التبدل في مناهجها ونمط الحياه الوظيفيه ولذلك اجوبه * طالما تعودنا على استيراد الخبرات فلا باس من ان تكون مناهجنا عباره عن استنساخ للمناهج العلميه الخارجيه وهنا يتم جلب محاضرين (لا ارسال موظفين في مناهج ترويحيه) يدربون الاساتذه على المناهج الجامعيه والبلدان تعج بالطاقات ومن انتهى عمره الافتراضي التقاعد اولى به. * الاساتذه يكونون مسؤولين عن تدريب مدرسي الثانويات على المناهج الجديده. * التخصص يبدأ من المرحلة الثانويه بعمر 15سنة دراسه 3سنوات قبل الجامعة بحيث لو اكمل الطالب دراسته الجامعيه يكون معدل سنوات اختصاصه هو 7ويكون في عمر 22سنة لديه اختصاص.

* وزاره التخطيط تدرس احتياجات السوق وتؤمن 50% من الوظائف الجديده للخريجين الجدد سنويا مع اتاحة امكانيه العمل التطوعي لكسب الخبرات للطلبة.

* التكاليف لهذه العمليات يتم استردادها عند تقديم خدمات جيده فمالمانع مثلا من تكوين شركات مختصه في النمذجه الثلاثيه الابعاد وطرح امكانيه تعاقدنا مع شركات غريبه ويكلف اقل كما هو حال الصين مع استراليا وبعد حين توجد امكانيه انتاج افلام انيميشن والعباب او برامج كبرنامج الاوفس الذي تكلف نسخته الاحداث مئات الدولارات مما ينتج عنه دخل قومي ففي اوريا مثلا كانت ارباحهم من الخدمات الالكترونيه لعام 2009مبلغ 500مليار يورو.

هناك كثير من الخطوات التي تسهم في تحسين الاقتصاد للدول وايجاد فرص جديده وتطوير المستوى العلمي العام وكل هذا سيساهم في انحسار كثير من مظاهر الفقر والتخلف والضياع.

محمد التميمي

فهل من مستمع ؟

موقع المجلة

www.networkset.net

بريد المجلة

magazine@networkset.net

جميع الحقوق محفوظة لكاتبها

محتويات تموز 2110



ماهي تقنية الـ Cloud Computing صفحة رقم 9

- | | | |
|----|----|---|
| 18 | 3 | - تعرف على عائلة سيرفرات نظام مايكروسوفت |
| 19 | 5 | - مقارنة بين سويتشات الطبقة الثانية والثالثة وMLS |
| | 6 | - من أين وكيف أبدا طريق الشبكات |
| | 7 | - ماهي الـ RFC وماذا تعني |
| 20 | 8 | - أهم المراجع والكتب الخاصة بدراسة كورسات جونيبر |
| 21 | 11 | - نتائج الاستفتاء الشهري |
| 22 | 12 | - كيف تقرأ أمر الـ Show Interface بأحترافية |
| 24 | 13 | - كيفية تحديد مشترك في الانترنت في WorkGroup ؟ |
| 25 | 14 | - كيفية إعطاء ويندوز XP أيبي V6 ؟ |
| | 15 | - كيف تتابع تغيرات الـ Routing Table |
| | 16 | - كيف تقوم بتأسيس شبكة فويس من الصفر |
| | | - خمس أشياء يجب أن تعرفها عن سويتشات سيسكو |
| | | - كيف تفهم أجهزة الطبقة الثانية Multicast ؟ |
| | | - قسم الأمن والحماية |
| | | - هجوم DHCP Starvation وطريقة التصدي له |
| | | - ماهو الـ Radius Server |
| | | - قسم عتاد ومعلومات |
| | | - قسم مصطلحات تقنية |
| | | - قسم مشاكل وحلول |



تعرف على عائلة سيرفرات مركز نظام مايكروسوفت (MS System Center Servers)

بقلم: محمد التميمي

تطوير وتوسعه الانظمة الحاليه.

- ★ توفير حلول امنييه جديده ومتكامله للاجهزه الحقيقيه والتخليه.
- ★ توفير حلول متكامله لخدمات النسخ الاحتياطي وحمايه البيانات مما يجعل بالامكان الاستغناء عن برامج النسخ الاحتياطييه الاخرى.
- ★ توفير الدعم لاداره السيرفرات الخاصه بالتعامل مع اجهزه الموبايل وتطبيقاتها.
- ★ توفير خدمات اداره السيرفرات التخليه والتطبيقات المتضمنه في تلك السيرفرات.
- ★ تحقيق منفعة اقتصاديه من خلال (اختصار تكاليف الاداره وتحقيق تكامل للبيانات والتطبيقات وامكانيه التخطيط السليم للتوسعات المستقبليه مما يقلل بالتالي من حجم المشاكل وحلول تلك المشاكل)



الاصدارات

1-Microsoft System Center Configuration Manager 2007

مدير تعريف مركز نظام مايكروسوفت , يستخدم لتقييم وتطوير وتحديث السيرفرات واجهزه الكمبيوتر الاعتيادييه وباقي الاجهزه القابله للتحديث كاجهزه الموبايل سواء كانت هذه الاجهزه حقيقيه او تخيليه (سيرفرات عائله الفيرتجول Virtual) ويعتبر الاختيار الامثل لتطوير السيطره على انظمه الـ IT.

2-Microsoft System Center Data Protection Manager 2007

مدير عمليات مركز نظام مايكروسوفت , يستخدم لاداره الخدمات المقدمه بأسلوب (End-to-End) ومثال هذا شركه تصاميم هندسيه تقوم بتنصيب نسخه برنامج التصميم الهندسي اوتوكاد 2010 على السيرفر الرئيسي ثم يقوم المهندسون من خلال اجهزه الكمبيوتر الخاصه بهم بالولوج الى التطبيق المتواجد على السيرفر في نفس الوقت (خاصيه التزامن) وهنا يتم تحديد نوعيه الخدمات المقدمه بالتفصيل كامكانيه اجراء عمليه المعالجه الصوريه باستخدام مصادر السيرفر من معالج وذاكره او على جهاز المستخدم نفسه.

لهذا يعتبر هذا النظام مساعد للمؤسسه لزياده الكفاءه من خلال اتاحه التحكم في بيئه الـ IT.

3-Microsoft System Center Data Protection Manager 2007

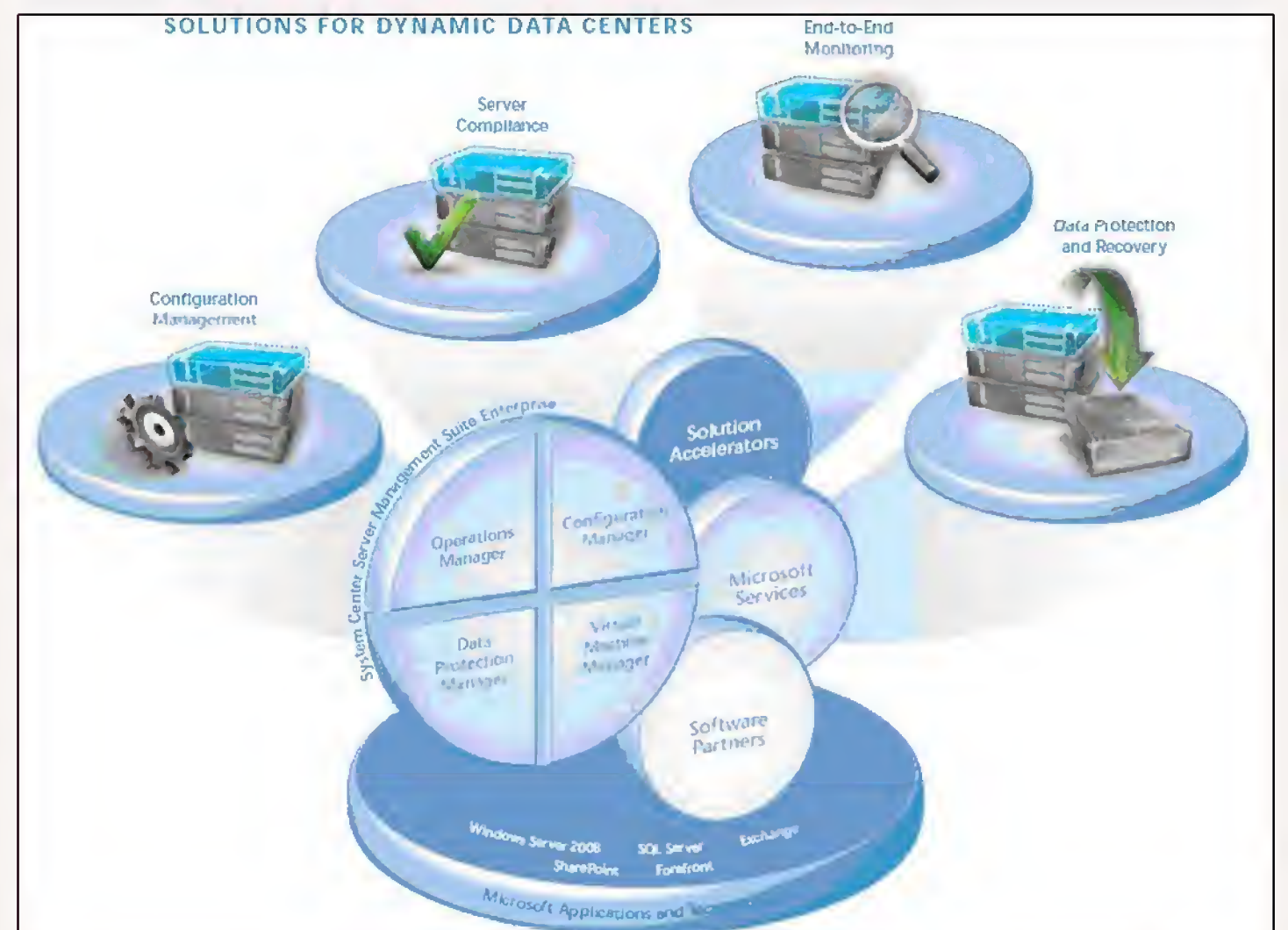
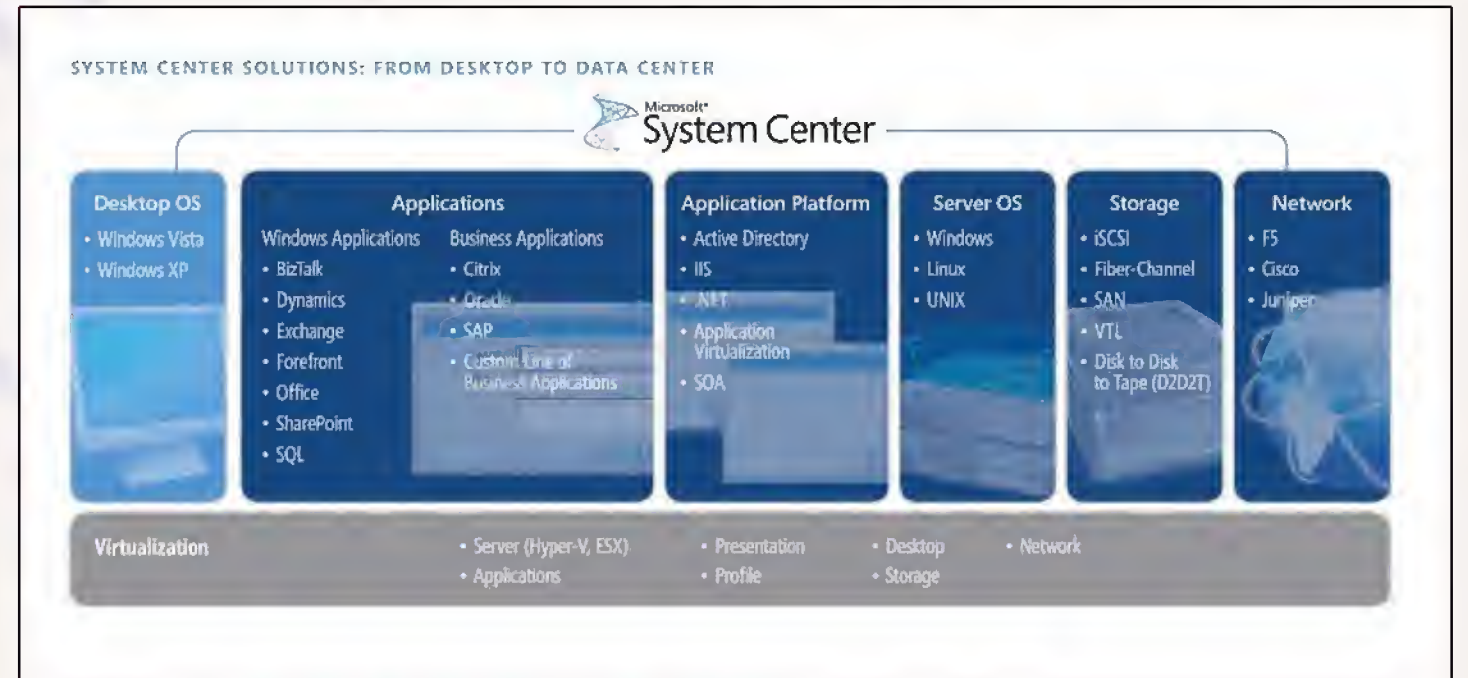
مدير حمايه بيانات مركز نظام مايكروسوفت , يستخدم كنوع من انظمه عمل النسخ الاحتياطييه للبيانات عبر الشبكه واسترجاعها وحمايه البيانات لتطبيقات المايكروسوفت ويدعم انظمه الـ (Raid) للاقراص الصلبه (Hard Disks) وباستخدام هذا النوع من انظمه الحمايه والنسخ الاحتياطي تننتفي الحاجه لاستخدام انظمه اخرى كالفيرتس او الاكرونس.

مع تنامي قدرات اجهزه سيرفر مايكروسوفت للشبكات المتوسطه وشبكات الانترنتبراييس (الكبيره) ظهرت الحاجه اكثر فاكثر الى نوع من السيطره المركزيه لاداره عمليات مهندسي ومديري النظم (System Engineers & Administrators)

لهذا دعت الحاجه الى ظهور هذا النوع من سيرفرات الوندوز والتي اصبحت منتجاتها الاخير (صدرت في 2007) من ضمن الاحتياجات الاساسيه التي يجب على مهندسي النظم اتقانها لا وبل الحصول على الشهادات الخاصه بها نظرا لتنامي الطلب عليها من قبل الشركات المتوسطه والعلاقه, حيث سنحاول في هذا التحقيق تسليط الضوء على الفوائد من استخدام سيرفرات هذه العائله وانواع الاصدارات الخاصه بها وهذا هو الجزء الاول من الموضوع على ان يتبع في الاعداد القادمه اجزاء اخرى تعنى بكل نوع من الاصدارات المختلفه بنوع من التفصيل.

ديناميكيه الـ IT

المقصود بهذا المعنى هو حيويه مديري النظم في اداره انواع مختلفه من المكونات الشبكيه وامتلاك نظريه مركزيه لتلكم الاداره , الان اصبح الامر ممكن من خلال اصدارات مركز النظام (System Center) والتي تتيح التعامل مع انواع مختلفه من الانظمه والتطبيقات كما هو موضح في الشكل الاتي



الفوائد

- ان نظره اوليه على الفائده التي يتم جنيها من خلال استخدام هذه الانظمه يمكن تلخيصها في الاتي
- ★ اداره مركزيه لجميع اجهزه السيرفر مع توفير ادوات متقدمه مما يسهل عمليه صيانه السيرفرات.
- ★ اداره مركزيه للتطبيقات المختلفه المقدمه من مايكروسوفت كخدمات البريد الالكتروني وقواعد البيانات مما يسهل عمليه اداره هذه التطبيقات وصيانتها.
- ★ توفير ادوات جديده ومتقدمه لمهندسي النظم لتطوير الخطط المستقبليه في



الخلاصة

حتى وقت ليس بالبعيد كانت هذه الانظمة في اصدارتها القديمة للعام 2005 غالبا مجرد انظمة تكميلية خاصة مع تفضيل الشبكات الكبيرة العمل على انظمة اللينكس , ولكن مع ظهور انظمة سيرفرات الوندوز 2008 وتحسن نوعيه الخدمات المقدمة اتاح هذا التطور اعتماده ووثوقيه اداء مما مكن من انشاء شبكات كبيرة تعتمد على انظمة مايكروسوفت لدعم عشرات الالاف العملاء , هذا التطور دعت الحاجة معه الى ايجاد وسائل ادارته وادوات ذات فعاله اكبر يتم اعتماده من قبل خبراء الانظمة لاداره وصيانته انظمتهم وهو ما قاد بالنتيجه الى مانراه اليوم من بروز متصاعد لانظمة الاداره المركزيه والمتمثله بعائله الـ MS System Center Servers.

4- Microsoft System Center Virtual Machine Manager 2007 يعتبر من الانظمة التي توفر , مدير الاجهزه التخيليه المركزي لنظام مايكروسوفت حلول اختصار التكاليف لاداره الاجهزه الحقيقيه والتخليه من خلال السماح باداره افضل للاجهزه التخيليه اضافه الى اداره السيرفرات الحقيقيه التي يحتضن كل منها عدد من الاجهزه التخيليه.

5- Microsoft System Center Capacity Planner 2007 . مخطط سعه مركز نظام مايكروسوفت , يستخدم لمرحلة تخطيط تطوير توسعه الشبكة المعتمده على انظمة مايكروسوفت خاصه حينما تكون هنالك تطبيقات متقدمه تعمل ضمن مجال الشبكة كخدمه البريد الالكتروني (Exchange Server 2007) وخدمه نقطه المشاركه (Windows SharePoint Services 3.0, and Office SharePoint Server 2007) وايضا خدمه مدير عمليات مركز نظام مايكروسوفت (Center Operations Manager 2007).

حيث توفر الادوات اللازمه والموجهات الضروريه لتطوير السيرفرات بكفاءه من خلال التخطيط المستقبلي وذلك بتحليل اداء السيرفرات في الوقت الحالي وبناء تقارير عن امكانيه السيرفر في احتضان تطبيقات معينه وماهي الحاجه للتطوير في عتاد السيرفر في حاله الحاجه لتوسعه التطبيقات الحاليه او المستقبليه.

6-Microsoft System Center Service Manager (Beta) . مدير خدمات مركز نظام مايكروسوفت , مصمم لانجاز الاحتياجات المتعلقه بمهندسي الدعم الفني (IT help desk) من خلال توفير ادوات متقدمه لاداره الحوادث والمشاكل المتعلقه بالمستخدمين النهائيين (Users) فهو باختصار نظام يتيح تطوير نوعيه الخدمات المقدمه للمستخدمين النهائيين من قبل فريق الدعم الفني.

7- Microsoft System Center Essentials 2007 .

اساسيه مركز نظام مايكروسوفت , عباره عن نظام مصمم للشبكات المتوسطة الحجم (300 سيرفر و 500 كمبيوتر) حيث يقوم بتوفير الادوات اللازمه لمهندسي النظم لاداره الشبكة وهو مشابه للنظام الاول الوارد ضمن هذا التقرير ولكن استخداماته متوفره للشبكات المتوسطة.

8-Microsoft System Center Mobile Device Manager 2008 . مدير اجهزه موبايل مركز نظام مايكروسوفت , يستخدم خاصيه منتجات (to-end) لتحقيق كفاءه تواصل وامنيه تناقل بيانات مابين اجهزه الموبايل وسيرفر خدمات الموبايل (Windows Mobile 6.1) والذي يوفر بدوره نقطه وصول واحده لجميع اجهزه الموبايل او مايعرف بـ (single-point access of LOB applications).

9- Microsoft Application Virtualization 4.5.

تخليه تطبيقات مايكروسوفت 4.5, يستخدم لتوفير مرونة التحكم بالتطبيقات التخيليه من خلال السماح لمديري النظم بانشاء واداره بيئه تخيليه تتحلل بسرعه الاداء وسهوله الاشراف على التطبيقات التي تتضمنها الاجهزه التخيليه, يتيح هذا النظام امكانيه الفصل مابين اداره اجهزه السيرفر التخيليه واداره التطبيقات المتضمنه ضمن تلك الاجهزه مما يوفر امكانيه تحكم اعلى في تلك الانظمة.

الطلب الوظيفي الحالي

في الدول الغربيه مثل امريكا واستراليا تم تركيز النظر على كل من (Configuration Manager Microsoft System Center 2007) و (Microsoft System Center Operation Manager 2007-2007) ضمن اغلب الطلبات الوظيفيه لمدراء ومهندسي النظم خاصه من قبل الشركات المتوسطة والعلاقه حيث ان اجاده هذين النظامين سويه والحصول على شهادتيهما من قبل مايكروسوفت يتيح مهارات اضافيه اصبحت اساسيه لخبراء الـ IT اضافه الى اجاده هذين النظامين معا يتيح زياده في الراتب السنوي تتراوح مابين 8 و 12 الف دولار

SWITCH

مقارنة بين سويتشات Layer 3, Layer 2 Multi layer

بقلم: أيمن النعيمي

تعد الفروقات بين السويتشات التي تعمل على الطبقات المختلفة أحد الأشياء التي تسبب الحيرة لبعض مهندسي الشبكات المبتدئين لذا سوف أطرح في هذا المقال أهم الاختلافات بين هذه السويتشات وخصوصا بين السويتشات التي تعمل على الطبقة الثانية والطبقة الثالثة مع توضيح فوائد استخدام السويتشات التي تعمل في طبقات أعلى والتي تعرف بـ Multi Layer Switch

LAYER-2

LAYER-3

LAYER-4

Layer 3 Switch

الكثير منا يصفه بأنه أشبه للروتر في عمله وأن كنت لا أتفق كثيرا مع هذا الكلام ولي عودة قريبه ان شاء الله لننتحدث عن الاثنين لذا أحب أن أقول عنه بأنه خليط من السويتش والروتر معا والذي يعطيه قابلية لكي يعمل كجهاز Layer 2 وجهاز Layer 3 والذي يعطيه كل المميزات التي ذكرناها في السويتش Layer 2 أما كونه Layer 3 فهذا يعطيه إمكانية ربط الـ Vlan's ببعضها البعض وتأمين اتصال بينها كون الموضوع مرتبط بوجود أيبي بالإضافة إلى إمكانية عمل Routing بين الشبكات باستخدام البروتوكولات المعروفة مثل RIP, OSPF كما تدعم هذه الأنواع من السويتشات الكثير من البروتوكولات الخاصة بتقنية الـ Voice Over IP والتي تحدث عنها الأستاذ أحمد الشحات في العدد الثاني من المجلة وأخيرا لتحويل المنفذ من Layer 2 إلى Layer 3 في أجهزة سيسكو نستخدم الأمر no switch port



CISCO-3560



Juniper-4200

وأخيرا هناك نوع ثالث من السويتشات يدعى Multi Layer Switch والذي يقوم بالنظر إلى طبقات أعلى من الطبقة الثالثة والتي قد تصل إلى الطبقة السابعة وله استخدامات كثيرة وأهمها توفير Load Balancing بين البروتوكولات مثل HTTP/HTTPS لتوزيعه على أكثر من سيرفر كما يمكنه اتخاذ قرارات بخصوص توجيه الترافيك اعتمادا على رقم المنفذ الموجود على الطبقة الرابعة أو يمكنه توجيه الترافيك معتمدا على نوع البروتوكول الموجود في خانة IP- Header والتي تحدثت عنها منذ يومين في تدوينة سابقة من خلال وضع جدول يحدد أرقام وأنواع البروتوكولات التي تكتب في خانة Protocol وأكثر ما يميزها هو الفعالية الكبيرة التي يعطيها لمدير الشبكة من خلال توفير خيارات كثيرة في إعداد أولويات تمرير الترافيك أو ما يعرف بـ QoS بسبب الخيارات الكثيرة المتاحة على كل طبقة أتمنى أن يكون الموضوع لهذا اليوم قد اجاب على الكثير من الأسئلة التي خطرت على بالكم وأن شاء الله سوف أقوم بطرح مقارنة بين الروترات والسويتشات Layer 3 في العدد القادم من المجلة فانتظرونا

Layer 2 Switch

قد يكون التحدث عن مزايا السويتش Layer 2 معروفة عند الجميع وكون الموضوع للمبتدئين سوف نتحدث عنه بشكل مفصل,بدأ هذا النوع من الأجهزة عملها في عام 1980 تقريبا (بحسب موقع سيسكو) وهي سويتشات مخصصة من أجل العمل على طبقة الـ Data Link Layer والتي تقوم بربط الأجهزة ببعضها البعض من خلال العنوان الفيزيائية لها أو كما يطلق عليه دائما Mac Address وكونه يعمل على الطبقة الثانية هذا لا يعطيه أي مميزات لفهم عناوين الأيبي لذا يعمل السويتش من خلال شبكة واحدة تقوم الأجهزة الأعلى منه مثل الروترات بتحديد ما يميزها عن باقي الأجهزة هو السرعة الكبيرة التي يقوم بتأمينها بين الأجهزة أو الـ End Device كون العمل يتم من خلال الهاردوير وعلى الطبقة الثانية فقط, أما عن آلية عمل السويتش فهي تعتمد على إضافة العنوان الفيزيائي الخاص بكل جهاز مرتبط مع السويتش من خلال أحد منافذ الـ Table خاصة تدعى Mac address table والتي يعتمد عليها السويتش في تحديد المنفذ الذي سوف يقوم بتمرير الترافيك إليه .

والميزة الثانية التي يملكها هذا النوع هو العدد الكبير للبورتات المتاحة والتي قد لا تجدها متوفرة أحيانا في السويتشات من نوع Layer 3 أو الروترات العادية ومن مميزاته أيضا إمكانية تقسيم المنافذ الموجودة عليه إلى أقسام منعزلة عن بعضها البعض باستخدام خاصية الـ Vlan والتي تؤمن بدورها حماية وأداء أكبر للشبكة والسويتش أيضا .

وآخر شيء هو ملاحظة أكثر مما هو ميزة وهو إعطاء السويتش أيبي ممكن في حالة واحدة وهي من أجل الإدارة والمراقبة وبكلام آخر يتم إعطاء السويتش أيبي لتمكين مدير الشبكة من الاتصال مع السويتش من خلال الـ Telnet وبالتالي إمكانية التحكم به عن بعد وبالتالي تمكين المدير من التحكم بشكل كامل فيه والاستفادة الثانية من إعطاء السويتش أيبي هو إمكانية مراقبة أداء وعمل السويتش من خلال بروتوكول الـ SNMP الذي يتيح لمدير الشبكة متابعة أداء السويتش عن بعد



CISCO-2950

Juniper-3200



D-link DGS-2208

3ComBaseline 2024



من أين أبدأ وكيف أبدأ في الشبكات؟؟؟

سؤال لطالما حيرني!!!

بقلم: عادل الحميدي



هناك موقع اسمه ebay وهو موقع موثوق به، والشراء منه يكون باستخدام الفيزا كارد، وهذا هو رابط الموقع:
<http://www.ebay.com/>

أدخل هذا الموقع وقم بكتابة CCIE Lab في محرك البحث الخاص بالموقع ستجد مفاجأة مذهلة في الأسعار، أولاً: CCIE هي أعلى شهادة شبكات في سيسكو سنتعرف عليها اليوم والتي تعني خبير شبكات، ثانياً: اللاب الخاص بـ CCIE إذا أحببت أن تشتريه جديد قد يكلفك كتييييييير جداً لكن هذا الموقع يبيع الأجهزة المستعملة الخاصة بالشركات الكبيرة والتي أحياناً قد تجد أجهزتها بشكل سنوي لذا ستجد الأسعار فيه أحياناً تصل إلى أقل من العشرة آلاف لعمل يحتاج مئات الآلاف، والأعجب والأجمل أنه بإمكانك أن تشتري قطعة قطعة كما تحب فعندما يتوفر معك أي مبلغ حتى لو 100\$ تقوم بالشراء، و CCIE Lab فقط مثال لكن الموقع مليء بكل تجهيزات الشبكات التي قد يحتاجها أي متخصص من الإبرة للصاروخ كما يقولون.

ولعل السبب في الرخص الشديد هو أن موقع ebay يعتبر أشهر مواقع المزادات على الإنترنت وأكبرها جميعاً، حيث يتميز بالعديد من السمات التي قلما أن توجد في موقع آخر، وهو يحتوي تقريباً على كل شيء يحتاجه الإنسان... قم بزيارة هذا الرابط:

<http://search.suhuf.net.sa/digimag/19092004/elc38.htm>

السؤال الثاني: هل أستطيع تحديد واختيار طريقي في الشبكات بنفسني؟ متى وكيف؟

الإجابة: نعم تستطيع، بعد سنة تقريباً (ممكن أقل ممكن أكثر)، سنة واحدة في المجال من العمل والدراسة والتدريب والتصفح، والمتابعة لكل ما هو جديد من خلال مواقع الإنترنت، كل ذلك سيأتى منه فهمك للمجال وللسوق واختيار الأنسب لشخصك وبلدك وطبيعة عملك في شركتك، وطبعاً بعد هذه السلسلة إن شاء الله ستجد الدنيا وردية بشكل أكبر لكن كن لنا متابع.

والآن لنرجع لإكمال المقالة... نقول بعد بسم الله وبعد أن انتهيت من الكورسين A+ و N+ تستطيع الاختيار بين مسارين:

الأول: سيسكو CCIE>CCNP>CCNA .
الثاني: مايكروسوفت MCP>MCSE>MCSA.

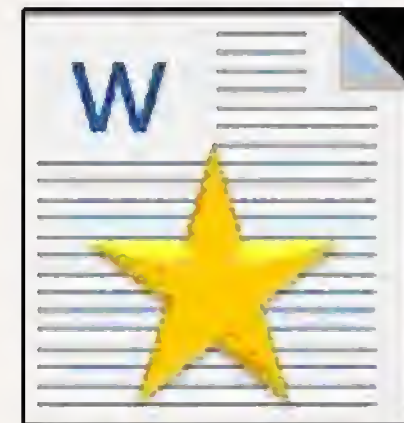
وقبل أن أبدأ في الكلام عن المسار الخاص بـ سيسكو ثم في المقالة القادمة عن مايكروسوفت، أريد التنبيه على أنه دائماً هنا ما نسمع السؤال التالي: أي المسارين أفضل؟ في الحقيقة المسارين حقيقة متميزين ولهما مستقبل باهر إن شاء الله، والذي يجب أن تعرفه من الآن أنهما ليس كما يشاع متعارضين، بل إنهما متكاملين... قد يتنافسا في بعض النقاط لكن لا غنى لأحدهما عن الآخر.

أذكر أنني كنت في أحد المؤسسات الحكومية 15 مبنى نريد عمل شبكة بينهم سويتشات وروتات سيسكو وفعلاً والله الحمد قمت بإعدادها وتمت بشكل ممتاز لكن كان هناك مشكلة في الإنترنت عجزت تماماً عن معرفة سببها، وفي آخر المطاف ظهر أن عندهم ISA Server (جدار ناري Firewall لحماية الشبكة ومتحكم فيها ومخزن مؤقت Cache لصفحات الإنترنت لتسريع التصفح) وكان هو السبب في المشكلة لكن لأنني كنت وقتها لا أعرف مايكروسوفت ما استطعت أن أحلها، وهذا الموقف حقيقة هو الذي حفزني على أن أدرس كورسات مايكروسوفت مع أنني أميل لـ سيسكو بشكل كبير وأنوي أن أكمل فيها...



أما اختيار بأيهما ستبدأ (لاحظ أنك في المسارين ستسير لأننا نبحت عن التميز)... يجب أن تعرف في كل شيء شيء وهذا ما يعرف بالثقافة يقال "إنسان مثقف"، "رجل IT" وهكذا.

كما تعودنا في بداية كل حلقة من تلك السلسلة (التي أسأل الله أن ينفع بها الإسلام والمسلمين) نجيب عن بعض التساؤلات والتي وصلتني على الإيميل خلال هذا الشهر والتي كانت هذه المرة قليلة جداً مقارنة بالمقالة السابقة، وفي اعتقادي أنها إشارة على أن المقالة السابقة كانت موفقة في الإجابة على تلك التساؤلات بشكل جيد.



واليوم بين أيدينا سؤالين فقط سأجيب عليهم لعلمي أنهم فعلاً سؤالين مهمين لا أدري كيف أغفلتهم وغابوا عني... ثم أكمل المقال، لكن قبل أن أبدأ أحب أن أشير إلى أنني وفيت بوعدي ورفعت لكم كورس اللغة الإنجليزية وفكرته مشروحة في سبعة أسطر لأن تلك الطريقة لها قواعد سبعة "7Rules Tips" أنصحك

أنصحك أولاً بسماعهم وقراءة الأوراق المرفقة بهم لكي تفهم الطريقة... ثم بعد ذلك أبدأ.

وهذا هو رابط لجميع الملفات: أهمها طبعاً قبل الأخير القواعد السبعة...
http://www.4shared.com/dir/MKXVX-YR/English_Course.html
تستطيع أن تجد الرابط أيضاً على مدونة Networkset

السؤال الأول: المواد التعليمية المتوفرة على الإنترنت في الشبكات هي كتب ومقالات وفديوهات وشروحات لكن كيف أتدرب عملياً وخصوصاً أن هذا المجال يحتاج للعملي أكثر من النظري؟!

بداية صدق أخونا في طرح هذا التساؤل فالمجال عملي أكثر منه نظري (لكن طبعاً النظري شيء لابد منه)، لذا فلتعلم أن لدينا طريقتين للتدريب العملي:

الأولى/ تعرف بـ Emulation، وهي تعني وجود معمل (لاب) مجهز بأجهزة كمبيوتر وأجهزة شبكات (سيرفرات سويتشات روترات وخلافه)، وهذا أمر صعب ومكلف جداً فوق ما تتخيل وقد تجده فقط في معاهد التدريب والشركات مع تحفظي على أجهزة الشركات لأنه لن يسمح لك بالتدريب عليها وإلا خربت الدنيا، باستثناء الشركات الكبيرة التي توفر لابات لتجربة أي شيء جديد قبل تنفيذه.

الثانية/ تعرف بـ Simulation محاكاة، وهي تعني برامج وهمية تخيلية تقوم بتحميلها على جهازك تساعدك على التدريب العملي، وهي متوفرة على الإنترنت.

لكن هناك تكنولوجيا جديدة تكلم عنها المهندس/ أيمن النعيمي في عدد شهر مايو من تلك المجلة يعرف بتقنية الـ Virtualization، وهي ببساطة جداً تعني برنامج تقوم بتحميله على جهازك (ذو المواصفات العالية طبعاً) فيقوم هذا البرنامج بأخذ جزء من الهاردوير الخاص بجهازك (جزء من المعالج CPU جزء من الذاكرة RAM وهكذا) ومن ثم تعطي هذا البرنامج نظام التشغيل الحقيقي للجهاز المطلوب عمله فيكونه لك، بالضبط كأنك اشتريته يعني بإمكانك مثلاً بناء وتكوين: سيرفر عن طريق برنامج VMware أو كمثال آخر يمكنك بناء وتكوين: سويتش وروتر عن طريق برنامج GNS، وفي هذه الحالة أنت فعلاً اقتربت من الطريقة الأولى لكن... أنا في اعتقادي أنك تحتاج فعلاً لبناء معمل (لاب) خاص بك، صدقتني إذا كنت تمتلك لاب خاص بك فعندها ستشعر بالفرق.

أعرف أن صدرك ضاق عندما قلت أنك تحتاج لبناء لاب خاص بك وخصوصاً بعد أن عرفت أن تكلفته عالية جداً لكن دعني أقول لك بعض أسرار المهنة أعطني أذنك...



الشهادة الرابعة: أما المستوى الثاني CCNP Cisco Certified Network Professional عليه مستوى الاحتراف ويأخذ حوالي 6 شهور ممكن أقل. وبهذا أنت أصبحت محترف في العمل على أجهزة سيسكو (سويتشات وروتات) والحمد لله الراتب يزيد يعني من 6 آلاف مثلاً ومع سنوات الخبرة التي تزيد أيضاً ممكن يصل إلى 12 ألف، أعرف شخص راتبه 18 ألف ريال سعودي معه شهادة CCNP وخبرة أكثر من 8 سنوات.

ويطلق عليه مستوى الاحتراف ويأخذ حوالي 6 شهور ممكن أقل.

وبهذا أنت أصبحت محترف في العمل على أجهزة سيسكو (سويتشات وروتات) والحمد لله الراتب يزيد يعني من 6 آلاف مثلاً ومع سنوات الخبرة التي تزيد أيضاً ممكن يصل إلى 12 ألف، أعرف شخص راتبه 18 ألف ريال سعودي معه شهادة CCNP وخبرة أكثر من 8 سنوات.

أما المستوى الثالث CCIE

"Cisco Certified Network Expert" مستوى الخبير، ولكن هذا المستوى ليس في خطتنا التي حددناها بالثلاث سنوات ولعله يأتي بعد ذلك... والله المستعان.

وقبل نهاية مقال هذا الشهر أردت أن أطرح سؤال -> من يستطيع أن يخبرني كم بقي الآن من الثلاث سنوات زمن الخطة؟؟؟

إلى اللقاء في الحلقة القادمة

تقرأون في هذه الحلقة ::::

كورس اللغة الإنجليزية 7 Rules Tips ...

كيفية التدريب العملي في مجال الشبكات...

بعض أسرار المهنة...

المسار الأول سيسكو: CCNA>CCNP

تقرأون في الحلقة القادمة ::::

المسار الثاني مايكروسوفت: MCP>MCSA>MCSE

وفي أيهما ستستمر حتى تكون خبير (لأننا نبحث عن التخصص والاحترافية)... يجب أن تعرف خبايا هذا الشيء وهذا ما يعرف بالتخصص.

أنا حقيقة لا أستطيع أن أقول ابداً بهذا المسار وتخصص فيه أو ذاك، وذلك لأن كل مسار له مميزاته وفرصه وعيوبه، كما أنه يتوقف على دولة الإقامة، والسوق المحيط بك ونشاط الشركات في تلك المنطقة لكن عموماً دعنا نضرب لذلك مثال... في مصر بلدي الحبيبة الأفضل كورسات مايكروسوفت فأنت إن حصلت على شهادتها قد تحصل على وظيفة بسهولة أكبر من كونك حاصل على شهادات سيسكو، أما في السعودية بلد إقامتي فاكشفت أنها على العكس تماماً فسيسكو فيها أفضل، لكن ليس معنى ذلك أنك لو حصلت على سيسكو لن تجد فرصة عمل في مصر، أو لو حصلت على مايكروسوفت لن تجد فرصة عمل في السعودية، كما أن الرواتب ومعدلاتها تختلف، فمثلاً في الغالب رواتب سيسكو تكون أعلى، والجهد في سيسكو أقل، لكن مايكروسوفت أسهل، وسيسكو أحياناً تكون معقدة، وللأسف ليس لهذه الأمور معايير ثابتة فقد يختلف البعض معي في هذا فكل إنسان يبني آرائه تبعاً لتجاربه ومشاهداته وخبراته وشهاداته والأمور التي مر بها في حياته، دعني أوجهك بتوجيهين كريمين...

الأول/ هو أن الموضوع أرزاق وتوفيق خذ بالأسباب وعليك بالسعي والله الموفق،

الثاني/ قبل أن تبدأ بأي مسار عليك بالاستشارة والاستخارة، استشير من حولك

ممن هم في التخصص وصل ركعتين استخارة وعندها اعلم أنك لن تندم "فلا خاب من استشار ولا ندم من استخار".

المسار الأول: سيسكو

الشهادة الثالثة: (بعد شهادتي +N, A) والبداية في

سيسكو تكون بكورس CCNA

Cisco Certified Network Associate

وكما اتفقنا ستكون لهذه الكورسات حلقات خاصة

نوضح فيها كافة المعلومات المتعلقة بمثل هذه الكورسات.

و CCNA تأخذ شهرين من طالب مجد مثل سعادتك... وهي تمثل المستوى الأول في سيسكو.

ماهي الـ RFC وماذا تعني ؟

بقلم: أيمن النعيمي

وبغض النظر عن المسمى الموجود عند كل بحث، للـ RFC عدة تصنيفات تحدد نوعية وتصنيف الموضوع وهي كالتالي :

Standard: وهي الأبحاث الرئيسية والهامة والتي لها التأثير الأكبر في تحديد المعايير والسلوكيات التي تعمل في الأنترنت مثل الـ

RFC 768 UDP, RFC 791 IP, RFC 1034 DNS

Informational: يعد التصنيف فقط كمعلومات عامة موجهة لتثقيف الناس فقط، وهي لاتعد معيار أو توصيات ينصح بها أمثلة عليها

RFC 1186 MD4 Message Digest Algorithm

RFC 1375 Suggestion for New Classes of IP Addresses

(وهو أحد الأبحاث التي قرأت عنها و كانت تهدف إلى زيادة عدد الـ Class المتاحة في IP v4 وطبعا هذا البحث كان قبل تأسيس الجيل السادس من الـ اي بي)

Experimental: يعد هذا التصنيف كدراسات تجريبية يقوم بها الباحثون وهذا

مثال عليها RFC 1339 Remote Mail Checking Protocol

Best current practice : يقدم هذا النوع من التصنيفات بعض المبادئ التوجيهية التي يمكن استخدامها مع المعايير الرئيسية Standard وهي بشكل عام

تعد أدارية أكثر مما هي عملية مثال عليها RFC 2026 والتي فيها تم إدراج موضوع التصنيفات هذه

Historic: فيها تدرج الأبحاث القديمة التي لم تعد تستخدم في الأنترنت أو تم تحديثها إلى إصدار أفضل ومن الأمثلة التي تحدثت عنها مسبقاً في موضوع الـ SNMP

بروتوكول CMIP الذي يحمل الرقم RFC 1189 Common Management Information Services

Unknown: يتضمن هذا التصنيف الأبحاث القديمة جداً والتي لم يعد لها مكان الآن في مفهوم الأنترنت الحالي

سؤال دائماً ما جال في خاطري ماهو الـ RFC وكيف بدأ وماهي فائدته وهو موضوعي لهذا اليوم الذي يهدف إلى أغناء المرجع العربي لهذا الحدث المهم في تاريخ الشبكات والأنترنت .

ماهو الـ RFC ؟

العني الحقيقي لهذا المصطلح هو Request for comments وهي سلسلة أبحاث علمية تصدر حالياً من خلال منظمة دولية تعرف بي Internet Engineer- ing Task Force أو IETF وتشمل هذه السلسلة أبحاث ومراجع علمية تقوم بتفسير سلوكيات عمل الأنترنت و الأنظمة التي تسيرها

وهي تتيح لمهندس وعلماء أجهزة الكمبيوتر بنشر أبحاثهم ضمن سلسلة منظمة وبشكل مرقم

تاريخ الـ RFC ؟

بدأت هذه الأبحاث ظهورها لأول مرة عام 1969 من قبل أحد مشاريع الأبحاث الأمريكية وتدعى ARPANET ولتتعرف أكثر على هذا المشروع قم بمشاهدة تاريخ الأنترنت

على الرابط التالي تاريخ الأنترنت

ونشر أول بحث تحديداً في 7 نيسان تحت أسم Host Software وقام بنشره حينها Steve Crocker من جامعة كاليفورنيا الأمريكية وليقوم بعدها في RFC3

بوضع أساسيات ما يعرف بي

Networking Work Group

ولتتوال بعدها الأبحاث العلمية وخاصة من جامعة كاليفورنيا مكان وجود منظمة ARPANET ولانها كانت أول من أمتلك تقنية Interface Message Processors



Juniper® NETWORKS

أهم الكتب والمراجع الخاصة بدراسة

شهادات جونيبر

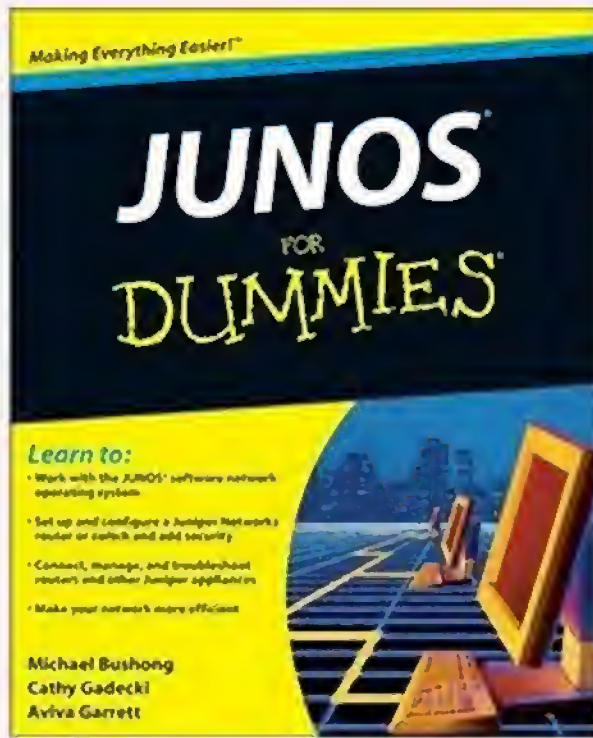
أعداد: أيمن النعيمي

النقطة الثانية وهي التدريب العملي وهو نقطة الضعف الموجودة في جونيبر فهي لم توفر أي برنامج يساعد على هذا الموضوع ولكن هناك بعض الأشخاص تمكنوا من عمل محاكي لاجهزة جونيبر يدعى OLIVE وهو شبيه ببرنامج GNS3 لكن إمكانياته ليست بقوة GNS3 ولكن يفي بالغرض في حال أنك لم تعمل أبدا على أجهزة جونيبر فهو يغطي الكثير من الأشياء في امتحان الروتر وللأسف لا يغطي أي شيء من امتحان السويتش وبالنسبة للسكريوتس لم اتطرق إليه وطريقة أعداده وتنصيبه موجودة على الرابط التالي

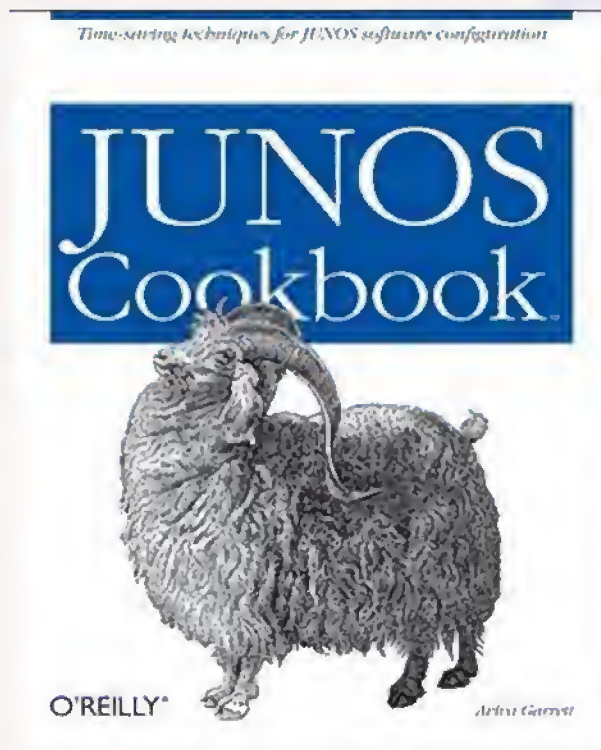
<http://www.networkset.net/2010/02/17/olive-juniper/>

أو قم بتحميل هذا الكتاب الإلكتروني الجاهز
<http://www.mediafire.com/?jjt2jmtwwij>

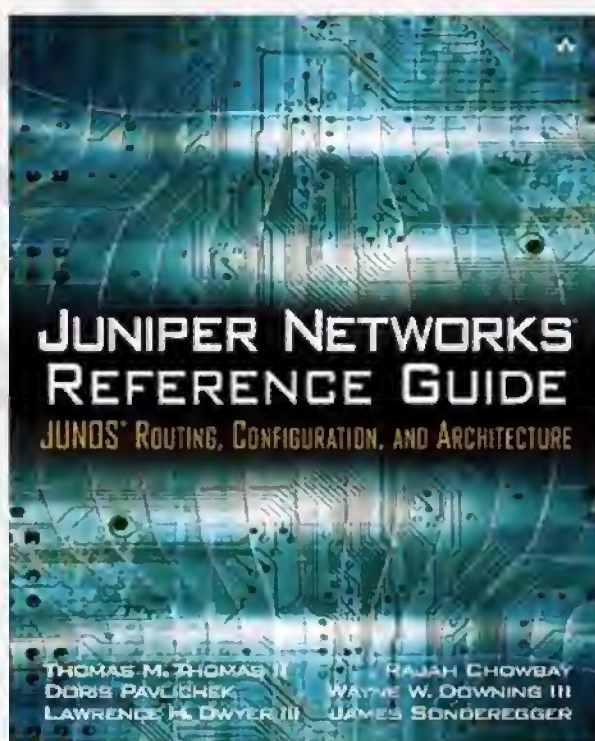
كما يوجد بعض الكتب والمراجع المفيدة والتي أنصح بها لدراسة جونيبر مثل كتاب Junos for dummies وهذه صورة للكتاب



وكتاب Junos Cookbook



وكتاب Juniper Networks Reference Guide Junos



بعد تعرفنا على شهادات جونيبر ومع اقتراب فترة إعلان جونيبر عن خصومات 100% على امتحاناته وان كانت جونيبر قد أرسلت لكل المشتركين معها رسائل تقول أن الخصومات بدأت إلا أن الموقع الرسمي لم يذكر أي شيء عن الموضوع لذا تدوينتي لهذه اليوم عبارة عن تعريف لكيفية تجهيز ودراسة مناهج جونيبر بالإضافة إلى مصادر الدراسة المتوفرة

ما قد لا يعرفه البعض بأن جونيبر قد أتاحت لكل دارسي شهادات جونيبر الموارد الكاملة بشكل مجاني وهذا يشمل الكتب الخاصة بكل شهادة بالإضافة إلى فيديوهات تعليمية في غاية البساطة وزد على ذلك امتحان تجريبي تستطيع من خلاله معرفة مستواك العلمي فيها ونتيجته تؤهلك للحصول على كود الفاجر (كود الخصم و100%) كل هذه الأشياء موجودة في صفحة واحدة وهي صفحة البرنامج التعليمي الخاص بجونيبر والتي أطلقت عليه Fast Track لتوجه إليه على الرابط التالي

<http://www.juniper.net/fasttrack/>

ولتطالعني واجهة الصفحة التالية

Existing Fast Track Program Participants		
The new Junos Security Certification Track is live with the addition of the Associate (JNCIA-Junos) Certification. Unless you already hold a JNCIA-ER or JNCIA-MS-ER certification, JNCIA-Junos is the pre-requisite to the JNCIS-SEC exam. Learn more		
Download archived JNCIS-ES Study Resources: Study Guide PDF , Lab Diagrams PDF , Lab Guide PDF		
If you were registered on the old portal, we have migrated your information. Sign in with your existing User ID and password.		
ENTERPRISE ROUTING CERTIFICATION TRACK	ENTERPRISE SWITCHING CERTIFICATION TRACK	JUNOS SECURITY TRACK
Associate (JNCIA-ER) Certification Steps: 1. Take the Junos as a Second Language eLearning course 2. Review Study Resources 3. Take the pre-assessment exam 4. Take the live exam at a Prometric testing center	Associate (JNCIA-EX) Certification Steps: 1. Take the Junos as a Switching Language eLearning course 2. Review Study Resources 3. Take the pre-assessment exam 4. Take the live exam at a Prometric testing center	Associate (JNCIA-Junos) Certification Steps: "pre-requisite for JNCIS-SEC exam 1. Take the Networking Fundamentals eLearning course 2. Review Study Resources 3. Take the pre-assessment exam 4. Take the live exam at a Prometric testing center
Specialist (JNCIS-ER) Certification Steps: 1. Take the Junos as a Second Language eLearning course 2. Review Study Resources 3. Take the pre-assessment exam 4. Take the live exam at a Prometric testing center		Specialist (JNCIS-SEC) Certification Steps: 1. Take the Junos as a Security Language eLearning course 2. Review Study Resources 3. Take the pre-assessment exam 4. Take the live exam at a Prometric testing center

نستطيع من خلال هذه الصورة ملاحظة 3 عواميد الأول خاص بموارد امتحان ال Router والثاني خاص بال Switch والآخر خاص بال Security وهي خمس امتحانات تدخل في عرض جونيبر الخاص بالخصم في العامود الأول نجد هناك شهادتان متاحان للروتر الأولى مبتدأ Associate والثانية مختص Specialist ونستطيع أيضا ملاحظة تحت كل شهادة هناك 4 ترفيقات وهي الموارد التي نحتاجها وهي بالترتيب التالي

- 1- شروحات بالفيديو للشهادة المعنية وهي عادة تأتي بعدة لغات مختلفة وطبعا العربية غير موجودة!
- 2- الكتب الخاصة بالدراسة وهي أحيانا تكون كتابان أو قسمان أثنان
- 3- امتحان تجريبي يؤهلك للحصول على كود الخصم
- 4- لحجز الامتحان وهو يتم من خلال موقع Prometric

وسوف تلاحظ مع أخي العزيز وجود قفل على كل من 2,3,4 والسبب هو عدم تسجيلك في موقع جونيبر لذا قم بالتسجيل الآن وأحصل على كل ماتريده من كتب وفيديو من جونيبر مباشرة ومجانا وطبعا تفس الشيء مع العامود الثاني والثالث



تعرف على تقنية الحوسبة السحابية Cloud Computing

بقلم: ياسر رمزي

يوجد 3 أنواع رئيسية من الخدمات يمكن توفيرها من قبل موفر الخدمة السحابية للعملاء (cloud services delivery models) أو XaaS :
Infrastructure as a Service IaaS
Platform as a Service PaaS
Software as a Service SaaS

الآن دعونا نتعرف بشكل بسيط على كل نوع :

Infrastructure as a Service (IaaS)



هي توفير تقنيات شبكية وعتاد و مراكز بيانات للعملاء و يتضمن هذا استخدام تقنية ال Virtualization و توفير نظم تشغيل يمكن الدخول اليها عبر الانترنت و يعتبر AMAZON EC2 من موقع امازون نموذج لهذا النوع و الذي يوفر حتى نظم تشغيل افتراضية و خدمات اخرى عديدة و كذلك نموذج اخر هو شركات ايجار الروترات و السويتشات لدراسي ال CCIE مما يخلق مصطلح الحوسبة عند الطلب او On Demand Computing .

Platform as a Service (PaaS)

وهي توفير كل ما يحتاجه المطورين لبناء تطبيقات و برمجيات و خاصة Web Based Applications من خلال توفير أدوات تطويره في بيئته قياسية standard .

منذ اسابيع قمت بعمل استفتاء في منتدى عرب هاردوير حول معرفة دراسي تكنولوجيا المعلومات بتقنية الحوسبة السحابية cloud computing وجاءت النتيجة مابين من لا يعلم عنها شئ او يعلم عنها تعريف فيه بعض الغموض وهذا التقرير سيحاول بشكل بسيط ان يضعك في بداية الطريق نحو هذه التقنية الهامة

لم يعد هناك شركة بفروعها الا و متصلة بالانترنت لتصبح شبكة الانترنت هي الوسيط الذي يربطها جميعا مع نفسها ومع الآخرين ومن هنا جاءت فكرة استغلال هذا الوسيط لتوفير خدمات مختلفه للشركات بفروعها المختلفه والموزعه على مستوى العالم وبالتالي مساعدة الشركات على توفير مبالغ ماليه ضخمة كان سيتم صرفها لتوفير تلك الخدمات داخليا بالشركة فمثلا كانت الشركة ستصرف هذه المبالغ على شراء معدات وبرمجيات وتوفير طاقم من المهندسين والمحترفين لصيانتها و ادارتها وبل حتى دفع فواتير التشغيل من كهرباء و الخ . مما كان يزيد التكلفة الاجماليه لامتلاك تقنية ما total cost of ownership TCO* .

أذن الحوسبة السحابية هي توفير خدمات مختلفه و متعددة للشركات عبر الانترنت و يكون الدفع حسب الطلب وحسب الخدمة المقدمة من موفر الخدمات هذه و الذي نسميه موفر الخدمة السحابية cloud service provider مما يعجل في ROI return of investments**

ويساهم بشكل كبير كحل من حلول معالجة الازمة الاقتصادية العاليه وتتوفر ال cloud في 3 اشكال هي private,public,hybrid ال cloud نفسها ما هي ال مجموعة hardware ,networks ,storage units ,software ,services يمكن توفيرها للعملاء من شركات مختلفه التخصص عبر الانترنت و كل هذا بالاضافه لما توفره الغيمه من قدرة على التوسع scalability حسب رغبة العميل في اي وقت و مرونة flexibility في الاداء حيث يستطيع موفر الخدمة بتوفير tracked (metered) لما يستخدمه العملاء لمعرفة المبالغ المستحقه عليهم .

ومن المتوقع ان خلال الفترة القادمة سيظهر جيل جديد من مواقع الانترنت نسميه الجيل الثالث او WEB 3.0 وستكون مواقع تفاعليه وخدميه اكثر تطوراً وسترتبط بالحوسبه السحابيه بشكل كبير مما قد يغير من مفهومنا لشبكة الانترنت .

أنهي هذا التقرير بمجموعة نصائح لشبابنا العربي العامل في المجال , عليكم بدراسة جيده لوسائل التخزين الشبكيه كـ SAN و تطبيقاتها على نظم ميكروسوفت و لينكس بمختلف نكهاته ومن أهم الشركات الموفرة لعناده هذه التقنيه شركة EMC الغنيه عن التعريف. عليكم بدراسة تقنية -Virtualization وخاصة ما تقدمه شركة vmware من حلول في هذا المجال بالاضافه طبعا لتقنيه hyper-v من ميكروسوفت وعلكم بدراسة حلول مقدمه لموفري الخدمه انفسهم حتى يستطيعوا تقديم خدماتهم مثل منصة Azure من شركة ميكروسوفت وكذلك عليكم الايام ببرمجيات ولغات تطوير المواقع المعتمده على الويب اذا كنتم مبرمجين ويب .

في تصريح لرمزي عيتاني مدير التوزيع بـسيمناتيك للحق تيلي بيزنس الصادر عن جريدة العالم اليوم الاقتصادي قال:

بحلول عام 2015 سيكون 20% من الشركات تعمل بمفهوم الحوسبه السحابيه ولكن نستبعد دخول المؤسسات المصرفيه و الكيانات الاقتصاديه الضخمه و الحكومات سبب مشكله ضعف تأمين البيانات في ال cloud و التي تعتبر نقطه الضعف الحاليه التي تعوق انتشار هذه التقنيه بشكل واسع.

ولقد استحوذت شركة سيمناتيك على شركة message lab

وهي الشركه المتخصصه في تأمين الحوسبه السحابيه و لديها موزعين في قطر و الامارات و السعوديه.

اهم الكتب بناء على تجربتي الشخصيه التي يمكن الاستزاده منها حول موضوع الحوسبه السحابيه :

Cloud Computing For Dummies - Robin Bloor & Judith Hurwi
ISBN-13: 978-0470484708

Roger Jennings "Cloud Computing with the Windows Azure Platform"

Wrox | English | 2009-10-05 | ISBN: 0470506385

بعض المواقع المفيده للتعرف على منصة ميكروسوفت الجديد:

Intro to the Windows Azure Platform

<http://bit.ly/aafTRm>

The Future of Cloud Computing with Business Productivity Online Standard Suite

<http://bit.ly/9vylgT>

A Beginners' Guide to Building the Foundation for a Cloud Computing Infrastructure

<http://bit.ly/aODUE6>

The Azure Services Training Kit

<http://bit.ly/91fxyL>

مصطلحات تم استخدامها و قد تكون غير مفهومه لدى القارئ :

★ Total cost of ownership TCO

التكلفه الاجماليه لامتلاك خدمه معينه او تقنيه معينه , تخيل معي تشتري عتاد بالف دولار و يحتاج موظف براتب شهري الف دولار لادارته وصيانته فهذا يعني شراء عتاد او برنامج بالف دولار و لكنه قد يكلفني في السنه 12 الف دولار لذا نقول عنه ال TOC له كبيره جدا

★★ return of investments ROI

كل مبلغ تصرفه الشركه كاستثمار مثلا في تقنيه ما تنتظر ان يعود بالكامل لخزينتها قبل انقضاء فتره معينه

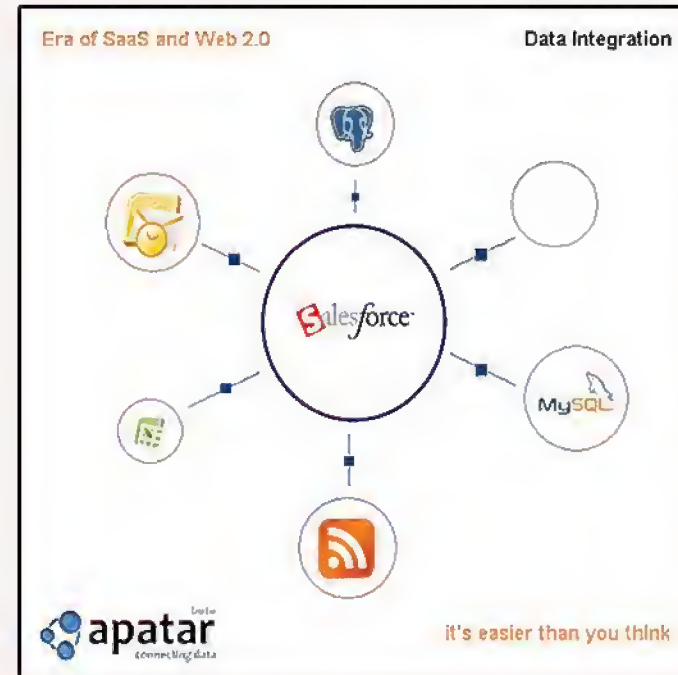
كلما تم تعجيلها كلما كان افضل و عموما هو مصطلح محاسبي اكثر مما هو تقني

ياسر رمزي عوده

مدير شركة CBTME للحلول التدريبيه بالامارات العربيه المتحده

Software as a service (SaaS)

و في هذا النوع نسمي موفر الخدمه السحابيه بـ ASP او Application Service Provider



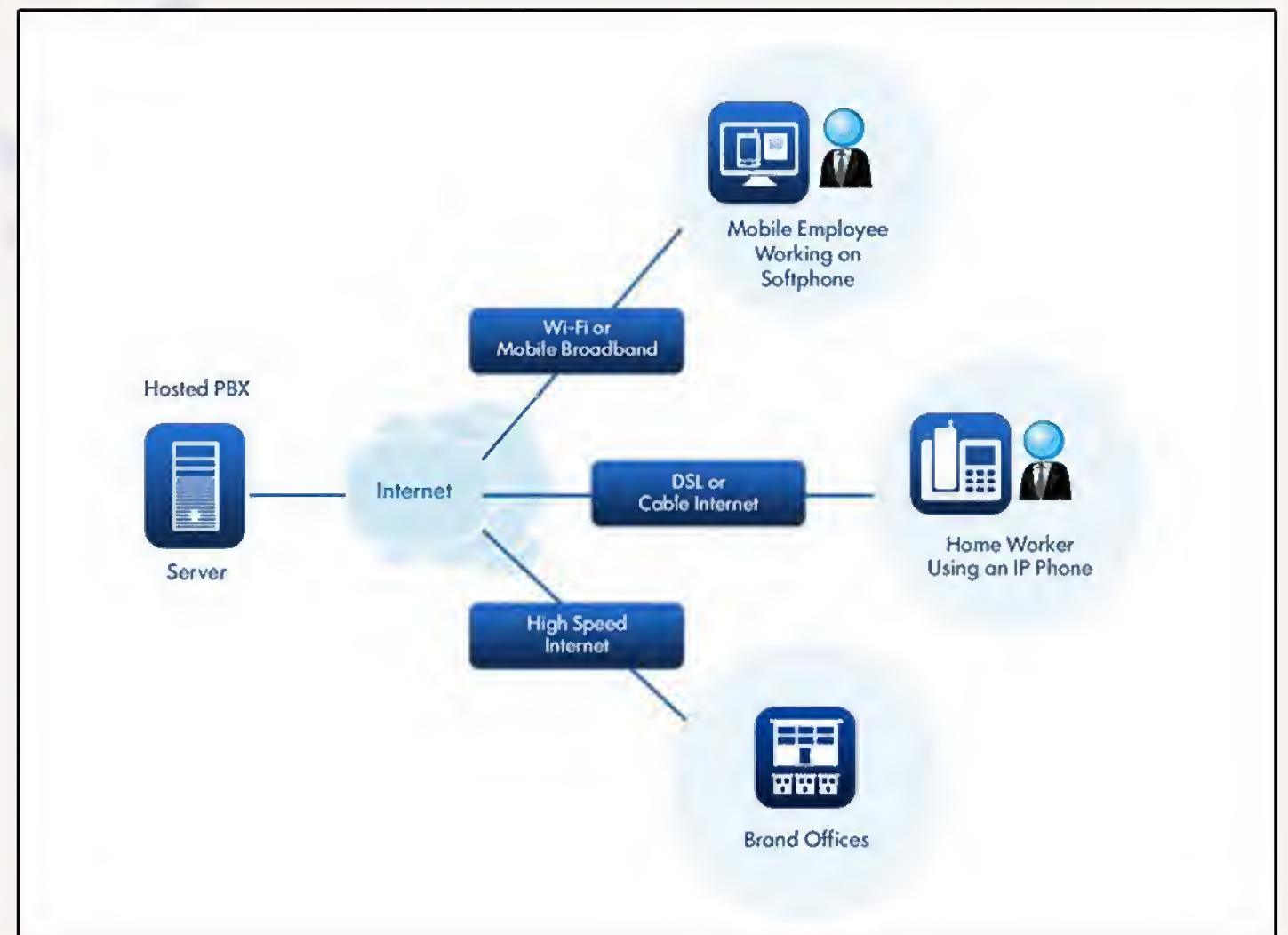
ويتم فيها توفير برمجيات إدارة علاقات العملاء CRM على سبيل المثال ويمكن اعتبار موقع salesforce.com نموذج لهذا النوع و مثال عليه و في الحقيقه يوجد نماذج اخرى عديده تعرفونها جيدا مثل FaceBook, eBay, Skype فمثلا الفيس بوك يوفر شبكه اجتماعيه للموظفين في شركه بدلا من استخدام برنامج خاص

على الشبكه الداخليه ليتبادلوا الاراء في امور العمل او تبادل ملفات العمل الهامه عموما في هذا النوع نجد حضور هام لتقنيات التأمين و اهتمام من ال ASP بتوفيرها بداخل خدماتهم لحماية بيانات العملاء عبر ال VPN وغيرها

وقد تم أيضا استحداث انواع اخرى للحوسبه السحابيه و منها على سبيل المثال وليس الحصر :

Communication as a service (CaaS)

وفيها يطلب العميل من موفري الخدمه بتعهيد Outsourcing حلول خدمات اتصالات , فمثلا توفير خدمات VOIP, real time presence, و خدمات المؤتمرات الفيديويه و على موفري الخدمه السحابيه من هذا النوع بضمان توفير جودة خدمه تطابق مع ال QoS المذكوره في اتفاقية مستوى الخدمه بين الموفر و العميل SLA service level agreements وضمان ادارتها بشكل مستقل عن قسم ال IT لدى العميل . يمكن اعتبار نموذج على هذا النوع حلول WEBEX من شركة سيسكو .



Monitoring as a Service (MaaS)

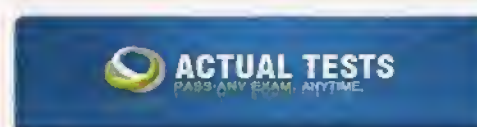
توفير خدمات مراقبه وحماية البيانات تتماشى مع متطلبات العميل والعمل بدوره قد يحتاج هذه الخدمات بناء على متطلبات حكوميه لنوعية الشركات التي يمثلها هذا العميل و يقوم موفر الخدمه هنا بتوفير باقات مختلفه للشركات منها توفير الاكتشاف المبكر لنقاط الضعف Vulnerabilities لدى العميل ونظم تشغيله .

اخيرا مجرد وجود صفحه للشركه (العميل) لدى موقع الفيس بوك هو تطبيق ونموذج للحوسبه السحابيه في أبسط صورها وساعدت الحوسبه السحابيه على التعجيل في الوصول لحل ل الازمه الاقتصاديه العالميه من خلال توفير مبالغ ماليه ضخمة كبيره على الشركات و في نفس الوقت توفير فرص عمل و دخل أكبر لشركات ال IT الموفرة للخدمات السابقة الذكر .

نتائج الأستفتاء الشهري



PassGuide
Make You Succeed To Pass IT Exams



في مداخلتي حول نتائج استفتاء هذا الشهر سوف أتحديث في أكثر من محور وسوف تتركز هذه المحاور على أسئلة كان يجب على أي شخص قام بالتصويت أن يطرحها على نفسه وبعد ما يقرر ما هو خياره الأفضل وخصوصا أن تحت خياران أثنان فقط ولا يوجد خيار وسط بينهم لاني أعلم أن الخيار الوسط سوف يأخذ أعلى نسبة في هذا التصويت لذا نتحدث بشكل أعمق.

السؤال الأول: من هو المستفيد الأول والآخر من وجود مثل هذه البرامج ؟

من خلال مشاهدتي لنتائج التصويت أنا واثق بأن أغلب المصوتين سوف يجابوا على هذا السؤال بأن الطالب هو المستفيد الأول وأنا أعتذر للجميع لأن هذا التفكير خاطيء 100% والسبب تستطيع أن تعرفه من خلال أجابتك على هذا السؤال هل تعتقد أن من الصعب على سيسكو أو مايكروسوفت أو أي شركة أخرى أن تحدث أسئلتها كل يوم وتصعب الأمر على الطلاب وعلى شركات مثل الباس فور شور ؟ الجواب لا والف لا لأن شركة مثل سيسكو بإمكاناتها تستطيع أن تضع كل ساعة أسئلة جديدة ولابات عملية مختلفة لكن سيسكو لم ولن تفعل ذلك لأن أغلبنا يعلم أن توجهات سيسكو في هذه الأمور هي توجهات تجارية بحتة وخصوصا أن أعداد الأشخاص الذين يدخلوا في امتحانات سيسكو بالملايين وهذه الملايين سوف تجلب لسييسكو المليارات من الدولارات لذا المستفيد الأول والآخر هي شركة **سييسكو والشركات التي تقوم بعمل هذه الأسئلة** والتي يدور محور الاستفتاء عليها لذلك الجواب الأول على هذا السؤال خطأ.

السؤال الثاني: من هو الخاسر الأكبر من وراء وجود مثل هذه البرامج ؟

نعم أخي العزيز أعتقد أنك قد عرفت الإجابة وهي **أنت** بكل معنى الكلمة لأنك أنت من يدفع النقود لسييسكو وهذه الشركات ولأن دراستك لأي شهادة لن تكون في المستوى المطلوب ولا تحاول أن تقتنعني أبدا بأن جاهزيتك للامتحان سوف تكون بنفس الطريقة وهذا الشيء التمسته من تجربة شخصية عندما قمت بدراسة وامتحان شهادة التريل شووت الجديدة من سيسكو فبسبب عدم وجود أي برامج مساعدة في هذه الشهادة قمت بقراءة كتابان حول هذه الشهادة وأحد الكتب والذي يحوي 700 صفحة تقريبا قراته مرتان وكلمة بكلمة مع تطبيق كل الأشياء التي تم ذكرها في هذه الكتب بالإضافة إلى مشاهدة الفيديوهات المخصصة لهذه الشهادة لذلك أجابتك على السؤال الثاني أخي العزيز أيضا خطأ.

السؤال الثالث: هل تعتقد أن توظيفك في أي وظيفة كانت سوف تتم من دون مقابلة شخصية ؟

أغلبنا يعلم بأن التوظيف في أي شركة لا يتم من خلال عرض الشهادات العلمية التي لديك إلا لو كان ابن صاحب الشركة فهذه حالة استثنائية لذا أخي ثق بأن هذه الشهادة سوف تكون لك فقط ولن تفيد أي أحد ومن هنا أحب أن أتوجه بكلمة مهمة لكل شركات التوظيف وهي أن لا تطلبوا للتوظيف أي شهادات علمية بل لكن الطلب هو شخص فاهم للشهادة ولا يشترط وجود شهادة علمية مع تعصيب فترة المقابلة لتشمل كل شيء يتعلق بهذه الشهادة وأكد أنتم والطلاب المستفيدون من هذا الإجراء.

لذا أنا أقول بأن هذه البرامج لن تسبب لك إلا المضرة فهي مضیعة للمال ولا تجعلك تركز بشكل أكبر في الدراسة والاختلاف لا يفسد للود قضية ولكن شعارك **لا للباس فور شور** ودمتم برعاية الله .

شجع هذا النوع من المجالات بوضع أعلائك هنا



كيف تقرأ أمر الـ Show interface على أجهزة سيسكو بأحترافية لتحليل المشاكل

بقلم: أيمن النجمي

Full-duplex, 100M/s

أكثر مشكلة تحدث في الأيثرنت هو عدم تطابق حالة المنفذ مع الطرف الآخر أي أن يكون هذا المنفذ Full بينما الطرف الآخر هو half لذا النظر إلى هذا القسم من الأشياء المهمة جدا بالإضافة إلى التأكد من سرعة الكبل أو الـ Data speed وهو هنا 100 M. هذا الحيز غير مهم لأكتشاف المشاكل وأنا أشرت إليه لأن كل الأرقام المكتوبة والتي تساعدك في تحديد المشكلة قد يتم إزالتها من خلال clear counter وبالتالي لن تستطيع تحديد المشكلة بشكل جيد لذا هذه الخانة تشير إلى آخر مرة تم إزالة الـ Counter الخاص بهذا المنفذ مثل أن نجد

Last clearing of show interface counters 00:20:42

ونستطيع أن نلاحظ أن العداد قد تم تنظيفه أو إزالته من حوالي العشرين دقيقة .

Input queue 0/75/0/0

أيضا من الأمور الهامة جدا وأهم رقم يجب مراقبته هو الخانة الثالثة الخاصة بي Drop والتي تشير إلى أن البورت يستلم بيانات أسرع من سرعة معالجتها على الروتر لذلك يبدأ في رميها والأسباب كثيرة مثل أن يكون المعالج مضغوط جدا من عدة مشاكل والتي سوف أتناولها في تدوينة أخرى حول أسباب ارتفاع أداء المعالج إلى مستويات أعلى من المسموح بها وهذا مثال يشير إلى وجود مشكلة مثل هذا النوع 77/75/200/0 ونلاحظ وجود 77 في Input queue و 75 تشير إلى أقصى عدد من الـ Packet يستطيع معالجتها ومن الخانة الثالثة نلاحظ أن الرقم يشير إلى 200 Packet . have been dropped

Output queue 0/40

نفس المبدأ السابق لكن هنا لا يوجد drop للبايت .

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

من هنا نستطيع أن نشاهد أحصائية تشير إلى عدد البايت والبت التي يتم نقلها في الثانية في آخر 5 دقائق وتستطيع تغيير الوقت الخاص بها من خلال الأمر load-interval وهذا مثال عملي عليها

30 minute input rate 624000 bits/sec, 254 packets/sec

30 minute output rate 571000 bits/sec, 231 packets/sec

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

تشير إلى مجموع الأخطاء التي حدثت في استلام البيانات والأسباب سوف تتوضح معك من خلال الأحصائيات الموجودة بعدها مباشرة مثلا مشكلة بسبب CRC أو Cyclic Redundancy Checksum والتي عادة تحدث بسبب عدم تطابق حالة الـ Duplex بين الطرفين ومن الأسباب أيضا هو frame وهي تحدث بسبب رقم البايت لا يتطابق مع الـ CRC بينما خانتها الـ overrun, ignored تحدث بسبب وجود مشكلة في البافر مثل انخفاض حجم البافر.

0 output errors, 0 collisions, 1 interface reset

وهي أيضا تشير إلى مجموع الأخطاء التي حدثت في إرسال البيانات والأسباب وجود تصادم في الكابل والتي دائما وغالبا مشاكلها بسبب الـ Duplex أو بسبب وجود مقويات كثيرة للأشارة repeater مع الطرف الثاني والخانة الثانية تشير إلى عدد المرات التي تم عمل فيها reset للمنفذ بسبب وجود بايت في الـ queue أو في الطابور.

0 Late collision

هذا القسم يشير إلى عدد المرات التي تأخر فيها الـ collision وهي تحدث عادة عندما تكون الشبكة كبيرة جدا والـ jam signal لا يستطيع الوصول إلى النهاية .

في هذه المقالة سوف أوضح كيفية قراءة أمر الـ Show Interface الخاصة بأجهزة سيسكو والهدف منها تحليل المشاكل التي حدثت على الروتر أو السويتش بشكل احترافي وسوف أبدا حديثي بعرض حالة أحد البورتات الموجودة وسوف اعلم باللون الأخضر على النقاط التي يجب النظر إليها في المقام الأول والتي سوف تساعدنا على تحديد المشكلة الرئيسية والتي قد تكون تؤدي إلى حدوث بطئ في الشبكة أو في نقل البيانات والذي قد ينعكس سلبا على أداء الشبكة بشكل عام

```
Router#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is cc00.0e00.0000 (bia cc00.0e00.0000)
Internet address is 192.168.10.1/25
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:00:02, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog
  0 input packets with dribble condition detected
 22 packets output, 7191 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
Router#
```

FastEthernet0/0 is up

أول شيء يقع عينك عليه في هذا الأمر وهو التأكد من أن المنفذ قد تم تفعيله وحالة الـ UP تشير إلى أن المنفذ تم تفعيله وبأنه يعمل بشكل جيد (ليس دائما) بينما حالة الـ Down تشير بنسبة 99% إلى وجود خلل في الكبل المربوط مع الطرف الثاني وأخيرا administratively down تشير إلى أن المنفذ مغلق ويجب تشغيله من خلال الأمر No shutdown

Line protocol is up

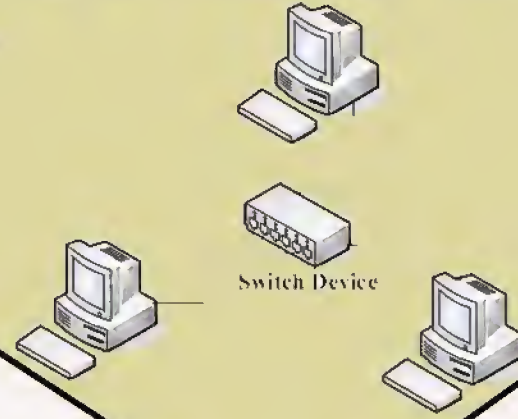
في هذا المكان يشير الأمر up إلى أن كل شيء على مايرام بينما حالة الـ Down في تقنية الـ Ethernet تكون بسبب وجود خلل في الطرف الثاني كأن يكون المنفذ مغلق أو أن يكون هناك خطأ في أعداد الطرف الثاني من المنفذ وتخبرك سيسكو بأن المشكلة بسبب الـ line protocol software processes have determined that the line is unusable. وتنصحك في حال وجود مثل هذه المشكلة بتغيير الكابل أو فحص الطرف الثاني من الكابل للتأكد من أن كل شيء على ما يرام (ملاحظة: نحن نتحدث عن الأيثرنت وليس عن السيريال)

Reliability 255/255

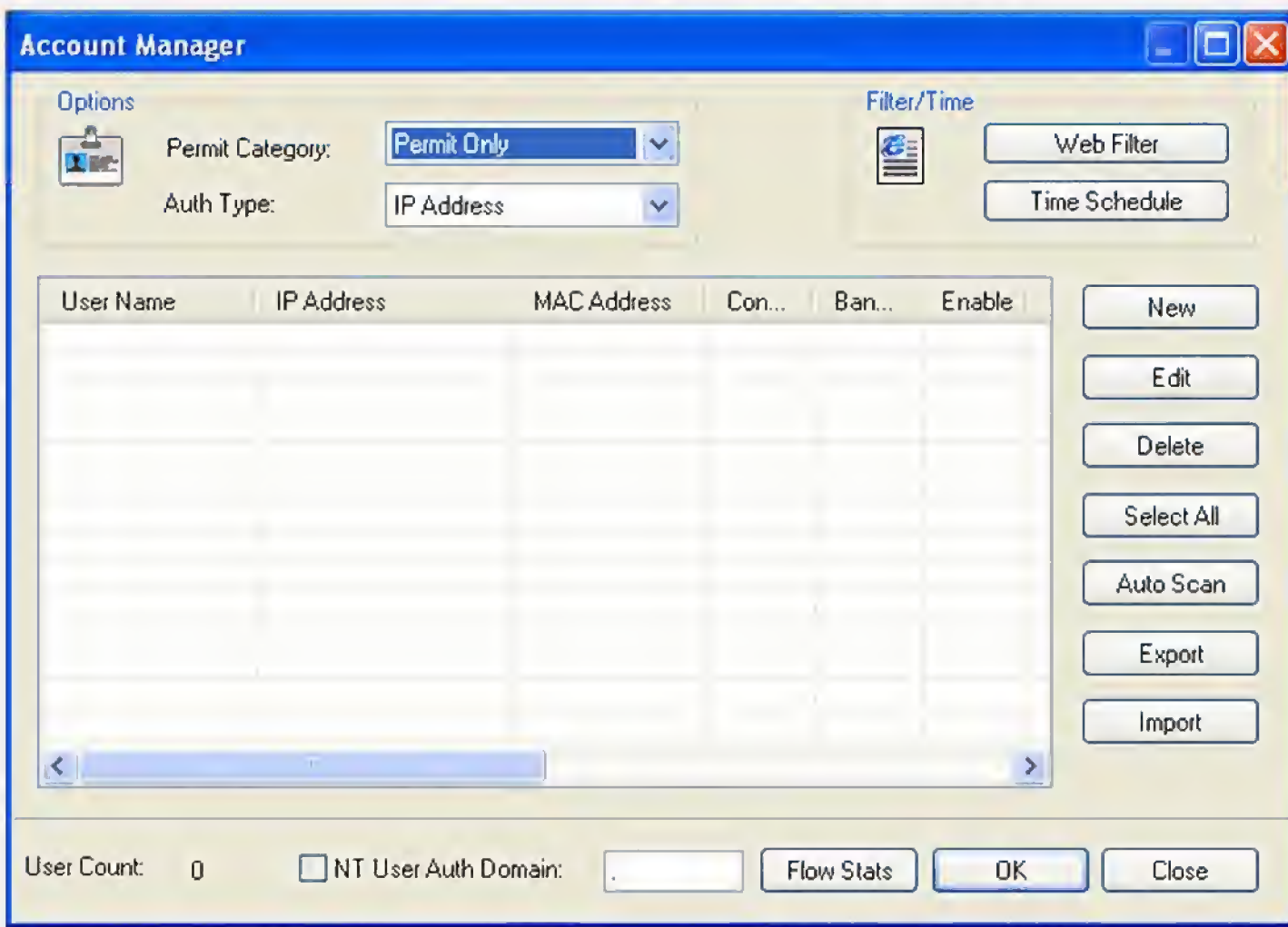
معنى هذه الكلمة هو الصلابه أو المتانة ويدل الرقم 255/255 بأن المنفذ في أفضل حالته وبأنه يعمل بشكل جيد ويحسب هذا المعدل كل خمس دقائق وانخفاض هذه النسبة دليل على وجود خلل في الطبقة الأولى أو الثانية مثل أن تكون الأرقام 255/235.

كيفية تحديد مشتركى الانترنت في شبكة WorkGroup

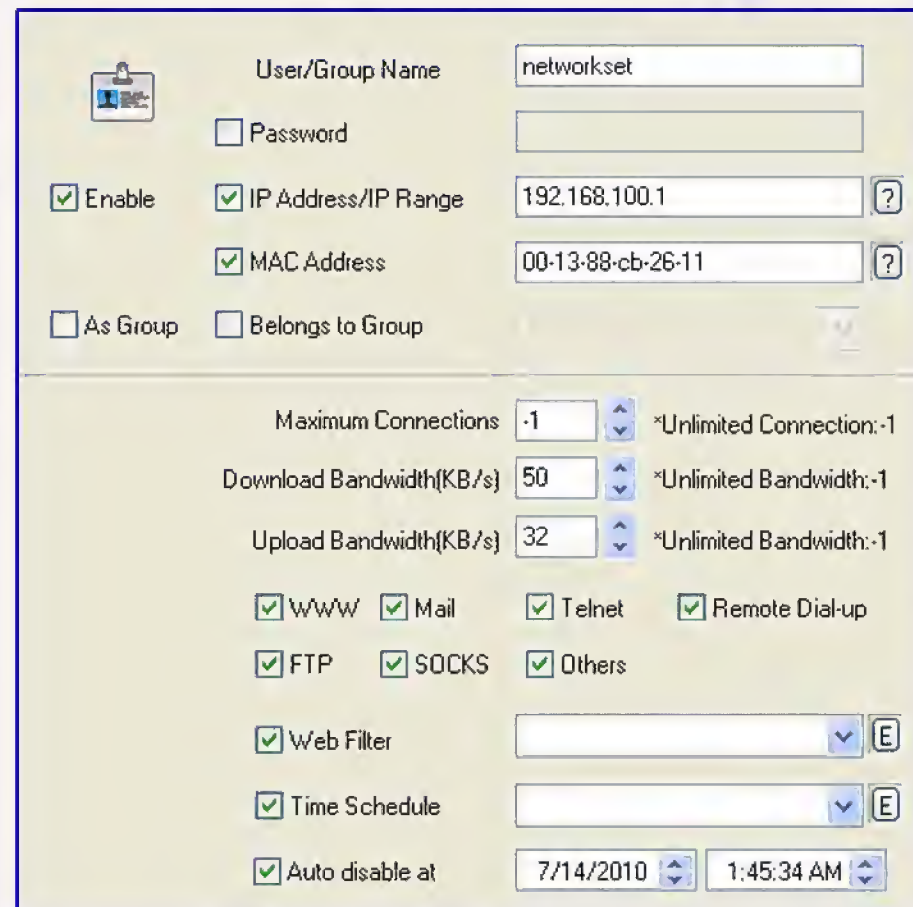
بقلم: أيمن النعيمي



من خلال هذه النافذة نستطيع أن نلاحظ ثلاث عواميد الأول Proxy Services وهو خاص بالخدمات التي تريد السماح لها بالعمل عند أجهزة العملاء مع وجود بعض الخيارات الأخرى مثل تشغيل البرنامج مع أقلع الويندوز بالإضافة إلى إمكانية تفعيل ال Web Cashed من أجل حفظ الصفحات في الكاش تستطيع ان تتحكم بهذا الموضوع بشكل اكبر من خلال الخيارات المتقدمة الثاني Protocol وهو خاص بتحديد البروتوكولات التي تريد السماح لها بالعمل على أجهزة العملاء الثالث Port من اجل تحديد البورتات التي سوف تعمل عليها البروتوكولات التي قمنا بتحديدنا وأن كان أكثر ما يلزمنا منها هو أول بورت وهو الخاص بي HTTP و (https (Secure بعد عمل الإعدادات المناسبة وتحديد البروتوكولات التي نريد السماح لها بالعمل نقوم بالضغط على زر موافق وننتقل للخيار التالي وهو Account.



اول شيء نقوم به هو تغيير Permit Category إلى Permit Only من أجل التحكم بالأجهزة المراد إعطاءها أيبي لذا نقوم أولا بأضافة الأبيبات التي نريد السماح لها باستخدام البروكسي وذلك من خلال الزر New وهذه صورة توضيحية لكيفية أضافة أيبي والتحكم بأعدادته .

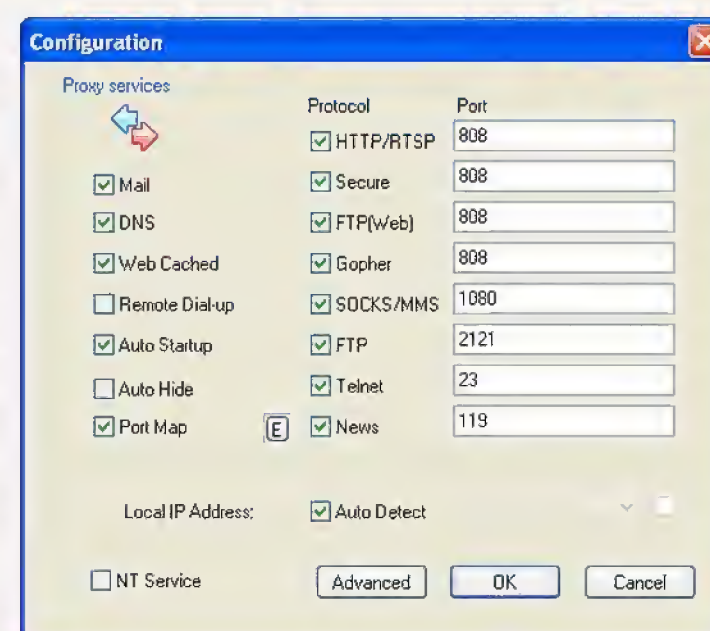
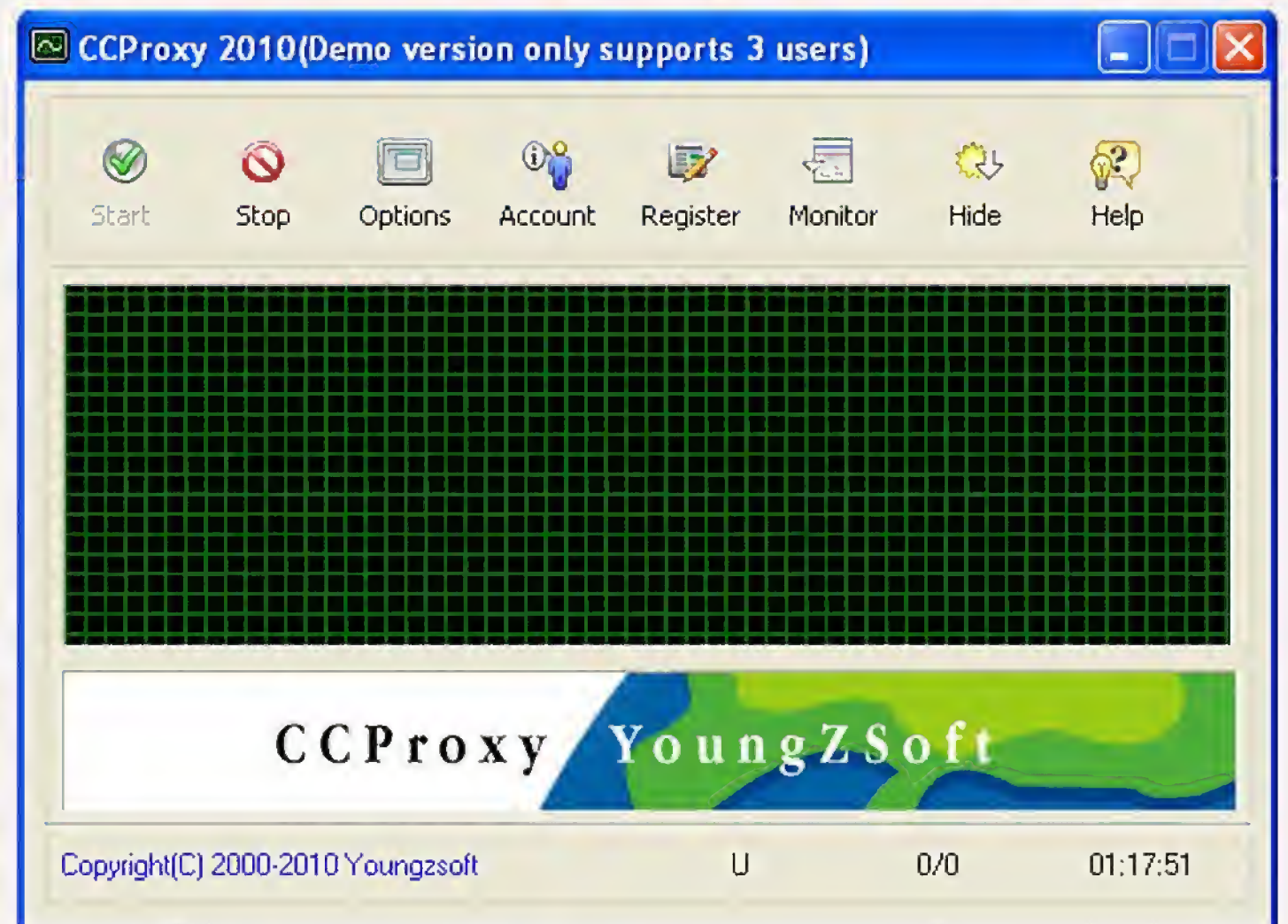


اول شيء نقوم بكتابة الأبيبي الخاص بالجهاز المراد السماح له باستخدام البروكسي والماك أدريس الخاص به وبعدها نستطيع أن نحدد أقصى عدد لل Connections المسموح بها وطبعا تحديد سرعة التحميل والرفع وتحديد الخدمات المسموح له بها (اختيار - أيعني عدد أو رقم غير محدد) وإذا كان هناك مواقع تريد أن تقوم بفلترتها تستطيع من خيار Web Filter وآخرها تحديد أوقات العمل المسموح بها وتحديد موقع أغلاق البروكسي على العميل أو المشترك لان البرنامج ممكن أن يفيدك في حال لو كان عندك شبكة وتقوم بتوزيع النت عليهم

قد تكون مسألة توزيع الأنترنت في شبكات الدومين من أبسط الأمور فهي عادة لا تتطلب من مدير الشبكة إلا تثبيت برنامج ال ISA Server من أجل التحكم بكيفية وطريقة توزيع الأنترنت على المستخدمين لكن لتتوقف قليلا ونطرح سؤال صغير كيف يتم بالتحكم بالانترنت على الشبكات الصغيرة من نوع WorkGroup وكيف أتحكم فيها بحيث أقوم بتوزيع الأنترنت على مجموعة معينة فقط وأمنع الأخرى ومن هنا أحببت أن اطرح بعض الطرق التي تساعدك على إدارة هذا النوع من الشبكات الطريقة الأولى تعتمد على الهاردوير والطريقة الثانية تعتمد على السوفت وير .

الطريقة الأولى : فكرته بسيطة جدا ولكن تحتاج إلى سويتش قابل للتحكم فيه أو Managed Switch وذلك من خلال الدخول على إعدادات السويتش والقيام بأغلاق البورت 80 والبورت 443 عن المنافذ التي لانريد السماح لها بالاتصال بالانترنت ولو في حال أردنا أن نتحكم بالبورتات المستخدمة بحيث نمنع أحدها سوف يتوجب علينا التوجه إلى الروتر المتصل مع الأنترنت وتطبيق بعض الأكسس ليست عليه وأنتهى الموضوع

الطريقة الثانية : وهي الطريقة التي قمت بتطبيقها في أحد الشركات وفكرتها ببساطة تتم من خلال استخدام برنامج بروكسي يدعى CCProxy وهو برنامج امكانياته كبيرة جدا من حيث تحديد البانديوث تحديد الأبيبات التي تريد السماح لها مع ربطها من خلال الماك أدريس وبالإضافة إلى Web cashed لتسريع التصفح وفلتره المواقع والكثير الكثير تستطيع تحميل البرنامج من موقع البرنامج على الرابط التالي <http://www.youngzsoft.net/ccproxy/> بعد تحميل البرنامج وتسطيبه على الجهاز نفتح البرنامج لنجد واجهة البرنامج التالية

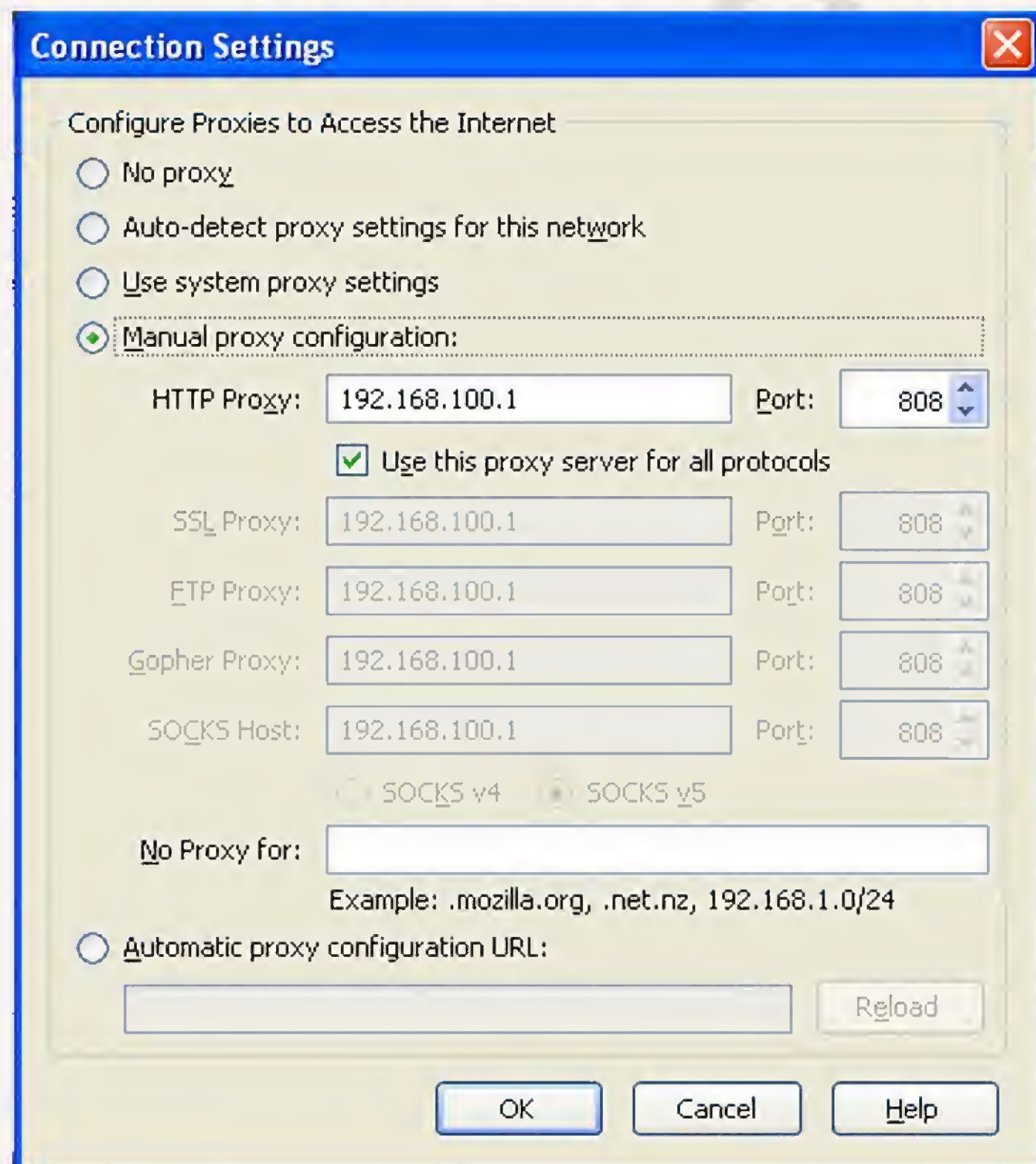


وكما يتضح لكم من الصورة أن البرنامج تجريبي ويسمح لثلاث أشخاص فقط استخدام البرنامج لذ فهو يحتاج إلى شراء مفتاح تسجيل من الموقع وأول خطوة سوف نقوم بعملها هي لأعداد Options الدخول إلى نافذة البرنامج لذا نضغط عليها لتواجهنا هذه النافذة

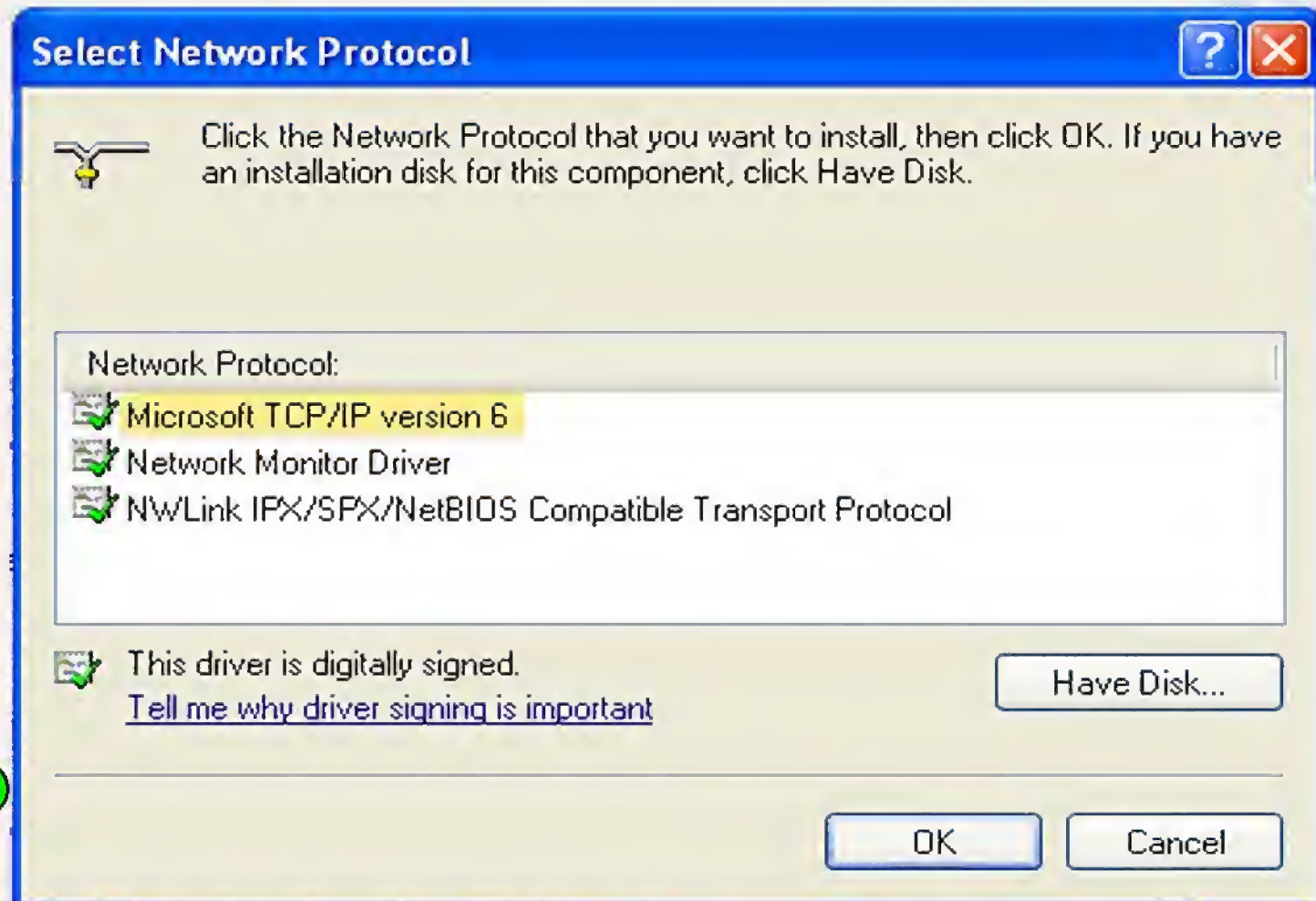
ونقوم بنفس العملية مع البرامج التي تحتاج اتصال مع الأنترنت مثل الماسنجرات كلمة أخيرة وهي إمكانيات هذه البرنامج كبيرة جدا وهذه لائحة بها باللغة الانكليزية :

- * Modem, Cable Modem, ISDN, ADSL, Satellite, DDN and so on are supported (more).
- * HTTP, FTP, Gopher, SOCKS4/5, Telnet, Secure (HTTPS), News (NNTP), RTSP and MMS proxy are supported.
- * Port Mapping is supported.
- * Web cache can enhance browsing speed. The size and refresh time of the cache can be easily changed.
- * Bandwidth control flexibly manages the traffic usage of clients.
- * Time schedule can easily control the clients' on-line time (access time control).
- * Web filter can ban the specified web sites or content, It can also name specific web sites for browsing.
- * URL filtering prevents users from downloading files with designated extensions via IE.
- * There are seven types of account authentication: IP address, IP range, MAC address, User Name/Password, IP + User Name/Password, MAC + User Name/Password and IP + MAC.
- * Parent proxy function enables CCProxy to access the Internet via another proxy.
- * Dial-On-Demand, remote dial up and auto disconnect are supported.
- * Access Logging can keep a full record of the Internet access log.
- * It enables IE and Netscape to access the Internet through HTTP/Secure/FTP (Web)/Gopher.
- * SOCKS5 proxy support allows use of ICQ, MSN Messenger, Yahoo Messenger, CuteFTP, CuteFTP Pro and WS-FTP.
- * Mail proxy supports Outlook, Eudora etc.
- * Supports NetTerm accessing the Internet via Telnet proxy.
- * Supports Outlook connecting to the News server via News proxy.
- * Support SOCKS5 and web authentication.
- * Support for Real Player RTSP proxy and Media Player MMS proxy.
- * Built-in DNS can resolve domain names.
- * Win98/WinMe/WinNT/Win2000/WinXP/Win2003/Vista compatible.
- * Bandwidth usage statistics.

إلى هنا نكون تقريبا انتهينا من إعداد البرنامج وبقي علينا خطوة واحدة وهي التوجه إلى جهاز العميل والدخول إلى إعدادات المتصفح وكتابة أيبي كرت الشبكة والذي يمثل ال gateway والذي قمنا طبعاً بتثبيت برنامج البروكسي عليه وتحديد البورت الذي قمنا بكتابته في البرنامج وهذه صورة توضيحية من متصفح فايرفوكس

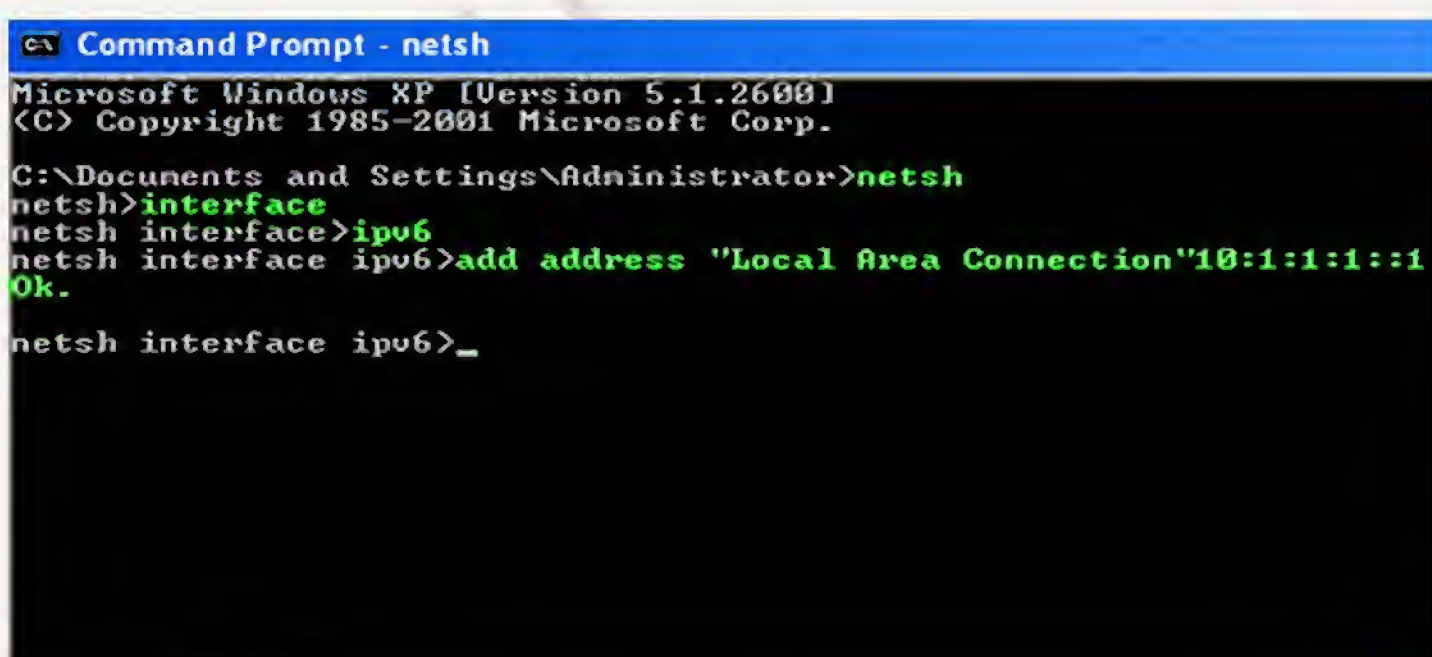


وبعدها نضغط على Protocol ونختار منها Microsoft TCP/IP Version 6 ونضغط أوكي لتحميل البروتوكول وبعد الانتهاء يجب عمل إعادة أقلاع للويندوز



لأعطاء أيبي 6 لأحد كروت الشبكة يجب علينا أولاً أن نقوم بعمل كوبي لأسم الكرت مثلاً "Local Area Connection" وبعد ذلك نقوم بتشغيل موجه الأوامر CMD ونقوم بكتابة الأمر netsh وبعد ذلك interface وبعد ذلك ipv6 وبعد ذلك نكتب الأمر التالي add address (NIC Name) ipv6

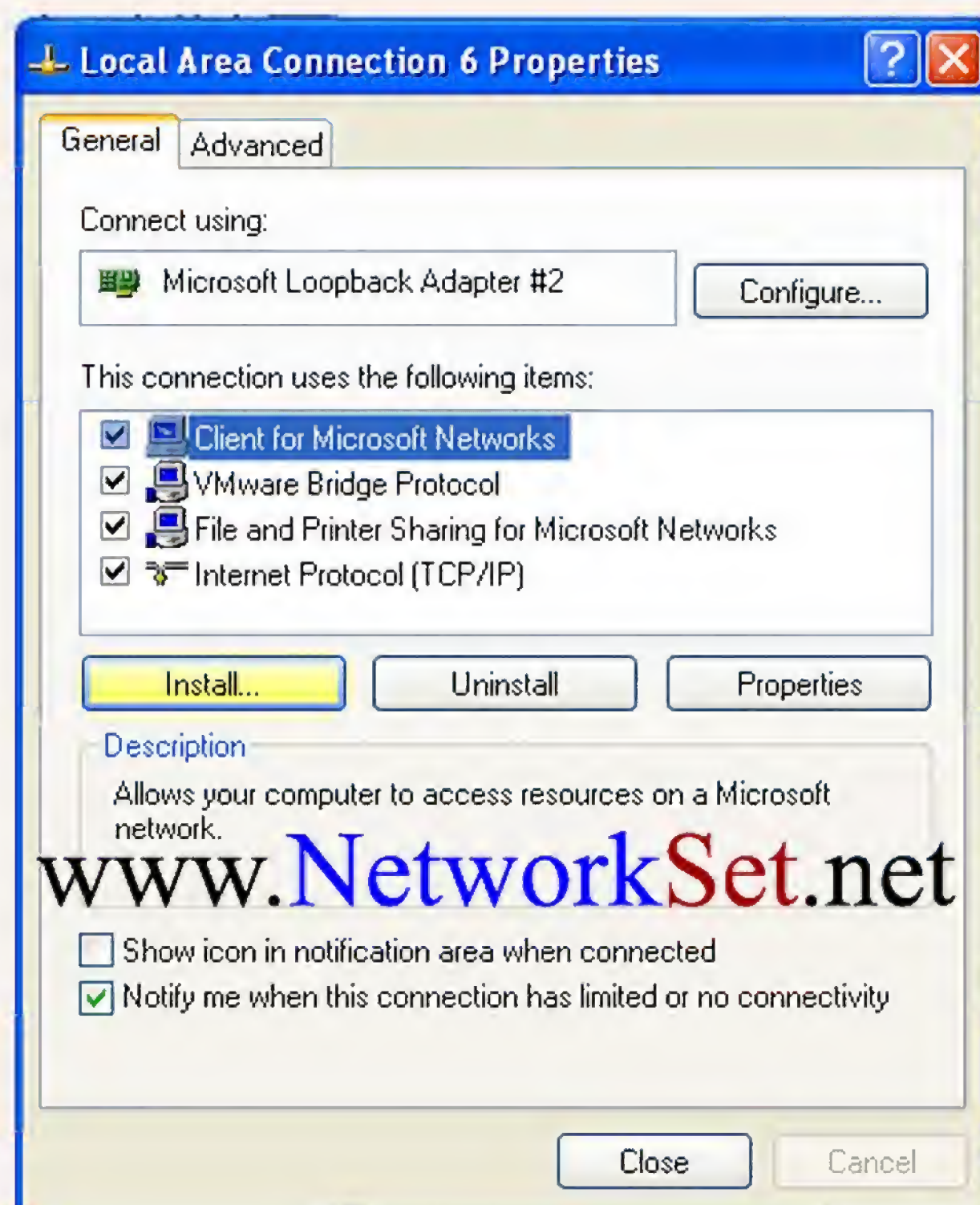
مابين القوسين نضع اسم كرت الشبكة الذي نريد عطاءه أيبي وبعد ذلك نكتب الأمر وهذا مثال يوضح كل الأوامر



كيفية إعطاء ويندوز أكس بي IPv6

أثناء إعداداتي لأحد اللابات الخاصة بي IPv6 أستوقفني شيء صغير وهو إعطاء أيبي 6 لويندوز أكس بي وقد اعتقدت أن الأمر بسيط جداً ويشبه طريقة كتابة أيبي 4 إلا أنني تفأجأة بأن أكس بي لا يدعم كتابة أيبي 6 من خلال واجهة الجرافيك GUI ولأعطاء أيبي لأحد كروت الشبكة نقوم بالخطوات التالية

أول خطوة سنقوم بها هي تثبيت بروتوكول الأيبي 6 على الجهاز وذلك من خلال التوجه إلى أحد كروت الشبكة والدخول على خصائص أو Properties وبعد ذلك نضغط على Install كما هو موضح بالصورة



كيف تتابع تغيرات الـ Routing table خطوة بخطوة

أثناء دراستي لكورس Troubleshooting تعرفت على أحد الميزات التي قامت سيسكو بأضافتها إلى نظام التشغيل 12.0 بعدما كانت من الأشياء المخفية في موجه الأوامر في الإصدار 11.0 وهو الأمر ip route profile يقوم هذا الأمر بمراقبة وتسجيل كل التغيرات التي تحدث على الـ Routing table وبالتالي تتيح لمدير الشبكة مراقبة التقلبات التي تحدث على الجدول مثل توقيت حدوث انقطاع في الشبكة والكثير من الأشياء التي سوف نتعرف عليها لذا لنقوم أولاً بتفعيل هذه الميزة من خلال التوجه إلى configuration mode وكتابة الأمر التالي :

```
Cisco's IOS
Router(config)# ip route profile
```

وبعدها نقوم بكتابة الأمر التالي لعرض الإحصائيات الخاصة بهذه الميزة

```
Router# show ip route profile
IP routing table change statistics:
Frequency of changes in a 5 second sampling interval
```

Change/ interval	Fwd-path change	Prefix add	Nexthop change	Pathcount change	Prefix refresh
0	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
10	0	0	0	0	0
15	0	0	0	0	0
20	0	0	0	0	0
25	0	0	0	0	0
30	0	0	0	0	0
55	0	0	0	0	0
80	0	0	0	0	0
105	0	0	0	0	0
130	0	0	0	0	0
155	0	0	0	0	0
280	0	0	0	0	0
405	0	0	0	0	0
530	0	0	0	0	0
655	0	0	0	0	0
780	0	0	0	0	0
1405	0	0	0	0	0
2030	0	0	0	0	0
2655	0	0	0	0	0
3280	0	0	0	0	0
3905	0	0	0	0	0
7030	0	0	0	0	0
10155	0	0	0	0	0
13280	0	0	0	0	0
Overflow	0	0	0	0	0

أول الأشياء التي يجب أن نعرفها بأن ip route profile يقوم بفحص الـ routing table كل خمس ثواني ويقوم بتسجيل التغيرات على شكل خمس تصنيفات كما هي موضحة في المثال السابق تصنيف كل عامود وهي

Change/ interval: عدد التغيرات التي حدثت

Forward-Path Change: تشير هذه الإحصائية إلى المرات التي تم تغيير الـ Forward-Path

Prefix-Add: تشير في حال تم إضافة شيء جديد إلى الـ Routing table

Next-Hop Change: تشير إلى تغيير الـ next-hop

Pathcount change: تشير إلى عدد مرات التي تغيير فيه عدد المسارات على الـ Routing table

Prefix refresh: نفس مبدأ الثانية وهي من أجل التأكد من الـ Prefix

لنعرض الآن بعض الأمثلة ونحاول تحليلها من أجل فهم هذه الخاصية بشكل أكبر

المثال الأول

ماذا سوف نفهم من الرقم 41 في الصف 0 لتحليل هذه القيمة يجب علينا أولاً أن نقوم بضرب الرقم $41 \times 5 = 205$ لاننا أشرنا في بداية الموضوع أن هذه الميزة تنظر كل 5 ثواني إلى جدول الـ Routing وسوف نستنتج بأن المدة هي 3 دقائق ونصف تقريبا وكونها في الصف الأول والذي يمثل صفر كما هو موضح هذا يعطينا الأستنتاج التالي بأن الـ Routing table خلال ثلاث دقائق ونصف لم يطرأ عليها أي تغيير والسبب لان هذه

```
Router# show ip route profile
IP routing table change statistics:
Frequency of changes in a 5 second sampling interval
```

Change/ interval	Fwd-path change	Prefix add	Nexthop change	Pathcount change	Prefix refresh
0	41	41	41	41	41
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
10	0	0	0	0	0
15	0	0	0	0	0
20	0	0	0	0	0
25	0	0	0	0	0
30	0	0	0	0	0
55	0	0	0	0	0
80	0	0	0	0	0
105	0	0	0	0	0
130	0	0	0	0	0
155	0	0	0	0	0
280	0	0	0	0	0
405	0	0	0	0	0
530	0	0	0	0	0
655	0	0	0	0	0
780	0	0	0	0	0
1405	0	0	0	0	0
2030	0	0	0	0	0
2655	0	0	0	0	0
3280	0	0	0	0	0
3905	0	0	0	0	0
7030	0	0	0	0	0
10155	0	0	0	0	0
13280	0	0	0	0	0
Overflow	0	0	0	0	0

القيم جميعها تقع في الصف صفر لذا الأرقام الموجود في أول صف هي طبيعية جدا ولا تشير إلى أي تغيير قد حدث على الشبكة لنرى مثال من نوع آخر

المثال الثاني

من هذا المثال سوف نجد أن هناك تغيير واحد قد طرأ على العامود الثاني والثالث وقد استدلنا من ذلك من العامود الأول الذي يشير إلى الرقم واحد بينما رقم أثنان تدلنا على مقدرا الوقت التي طرأ فيه التغيير وهو $2 \times 5 = 10$ ثواني وهي حالة طبيعية ممكن حدوثها على الشبكة لكن لنشاهد المثال الثالث وعندها سوف نبدأ نفهم أكثر حول الموضوع

```
Router# show ip route profile
IP routing table change statistics:
Frequency of changes in a 5 second sampling interval
```

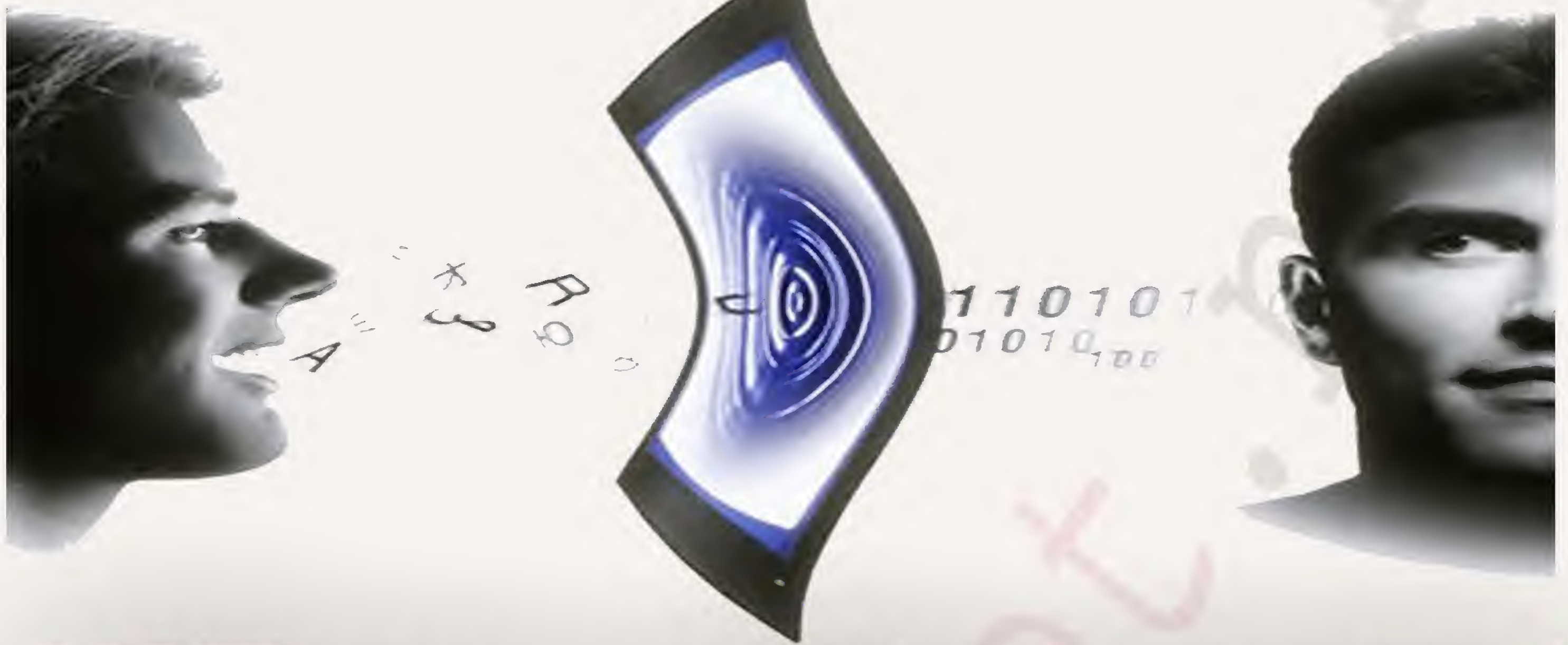
Change/ interval	Fwd-path change	Prefix add	Nexthop change	Pathcount change	Prefix refresh
0	39	39	41	41	41
1	2	2	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
10	0	0	0	0	0
15	0	0	0	0	0
20	0	0	0	0	0
25	0	0	0	0	0
30	0	0	0	0	0
55	0	0	0	0	0
80	0	0	0	0	0
105	0	0	0	0	0
130	0	0	0	0	0
155	0	0	0	0	0
280	0	0	0	0	0
405	0	0	0	0	0
530	0	0	0	0	0
655	0	0	0	0	0
780	0	0	0	0	0
1405	0	0	0	0	0
2030	0	0	0	0	0
2655	0	0	0	0	0
3280	0	0	0	0	0
3905	0	0	0	0	0
7030	0	0	0	0	0
10155	0	0	0	0	0
13280	0	0	0	0	0
Overflow	0	0	0	0	0

المثال الثالث

لندقق عند الرقم الثلاثين سوف نلاحظ أن هناك من 30 إلى 54 تغيير قد تم خلال خمس ثواني في كل من العامود الثالث والخامس والأستنتاج كان من خلال وجود الرقم واحد وهو كما أتفقنا يشير إلى خمس ثواني ولو كان مكتوب أثنان فهذا يعني بأن هذه التغيرات قد تمت خلال 10 ثواني وهذا الشيء طبعا خطير لان هذا العدد الكبير من التغيرات وفي زمن قدره خمس ثواني يدلنا على حدوث مشكلة في الشبكة ومن أشهر هذه المشاكل هو Routing loop

```
Router# show ip route profile
IP routing table change statistics:
Frequency of changes in a 5 second sampling interval
```

Change/ interval	Fwd-path change	Prefix add	Nexthop change	Pathcount change	Prefix refresh
0	39	39	41	41	41
1	2	2	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
10	0	0	0	0	0
15	0	0	0	0	0
20	0	0	0	0	0
25	0	0	0	0	0
30	0	1	0	1	0
55	0	0	0	0	0
80	0	0	0	0	0
105	0	0	0	0	0
130	0	0	0	0	0
155	0	0	0	0	0
280	0	0	0	0	0
405	0	0	0	0	0
530	0	0	0	0	0
655	0	0	0	0	0
780	0	0	0	0	0
1405	0	0	0	0	0
2030	0	0	0	0	0
2655	0	0	0	0	0
3280	0	0	0	0	0
3905	0	0	0	0	0
7030	0	0	0	0	0
10155	0	0	0	0	0
13280	0	0	0	0	0
Overflow	0	0	0	0	0



كيف تقوم بتأسيس شبكة فويس من الصفر (VOIP)

بقلم أحمد الشحات

كما تعودنا دائما يتكرر لقائنا في كل عدد من المجلة مع درس جديد سنتكلم الان عن بعض المصطلحات المهمة التي يجب أن يعرفها كل مهندس فويس طبعا وكما تعودنا فنحن لن نتكلم بتفصيل ممل عن كل شيء نحدده فنحن لا نشرح كورس دراسي بقدر ما هو تقريبا لفاهيم المهندسين المبتدئين لكي يساعدكم هذا الملف عندما يبدؤوا دراستهم العملية في الفويس

أشكال شبكة الفويس

موقع واحد فقط (site deployment single)

كلمة cluster تعني أكثر من جهاز يعملون وكأنهم جهاز واحد. وهنا تعني أكثر من سيرفر (كل واحد مستقل بذاته) يشتركون في بعض الخصائص وهي :

1- run-time data (intra-cluster communication signal) وهي متعلقة بتبادل المعلومات التي تسجل ديناميكيا وتحدث أثناء العمل ومن أمثلتها phone registration وأيضاً عند حدوث سقوط أحد ال CUCM تنتقل التليفونات تلقائياً لل CUCM الآخر

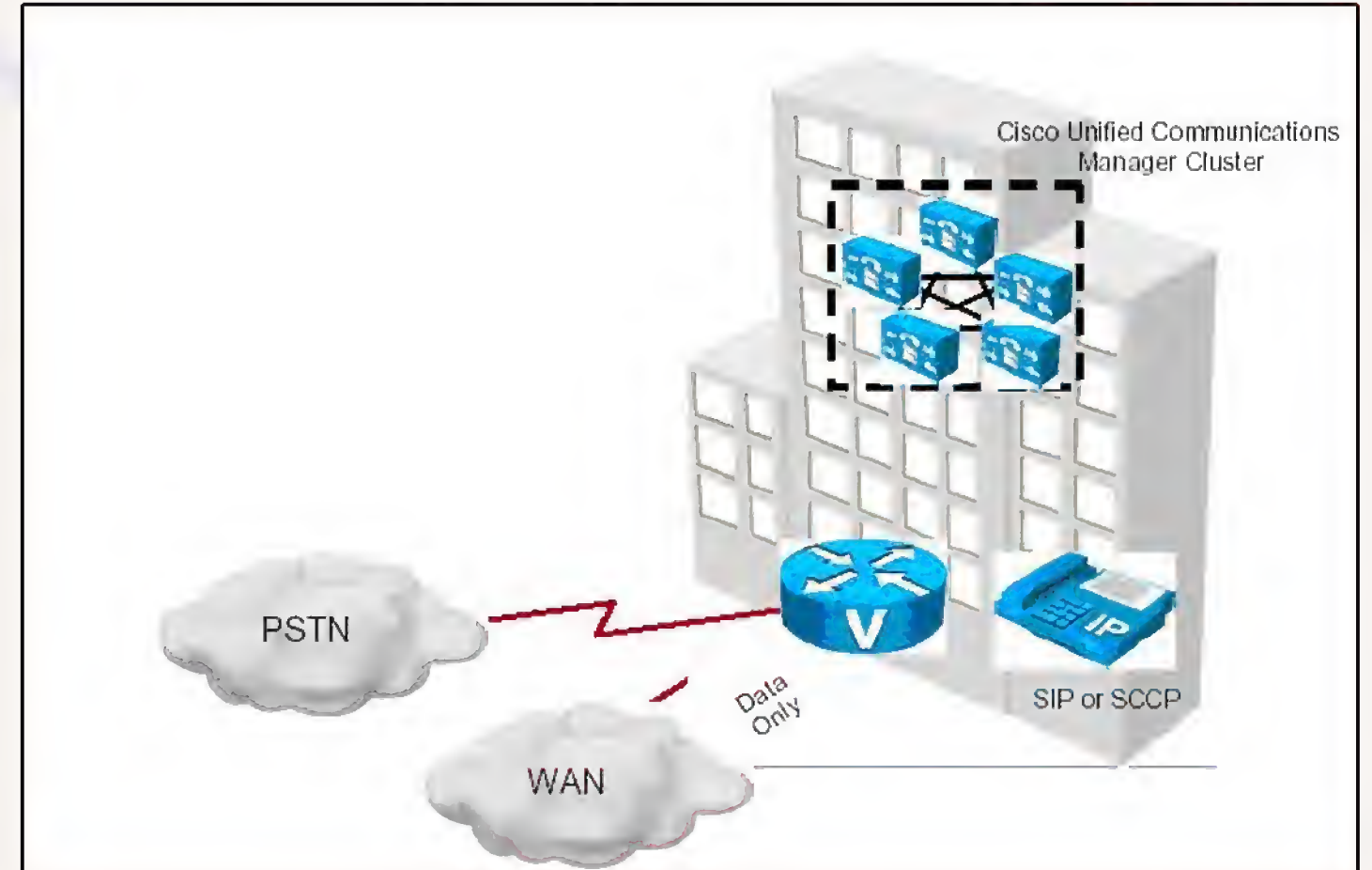
2- database data (ids database replication

حيث يتم تبادل قاعدة البيانات ككل بين السيرفرات من هذه المعلومات أرقام التليفونات والمالك الخاص بكل تليفون وال dial plane وغيرها ملحوظة : يمكن عمل أكثر من cluster داخل الشبكة المحلية او داخل MAN وربطهم مع بعض عن طريق Inter cluster trunk لو كان لدينا العدد أكثر من المسموح به

* هذا الشكل يدعم حتى H323 I100 جهاز وسنعرف فيما بعد ما هو البرتوكول h323 وقد اخذنا عنه نبذة فيما مضى ولكن في المثال العملي فيما بعد سنقوم بتهيئة الفويس راوتر بواسطة هذا البرتوكول

* طبعا كل الخدمات الاخرى متاحة في تلك الشبكة من بريد صوتي وغيره * من مزايا هذ الشكل انه لو سقطت IP WAN فان الشبكة لن تتأثر كما انه سنستخدم CODEC واحد لكل الشبكة G711 وفي هذه الحالة سيتم توفير DSP لاستخدامها في تطبيقات اخرى وليكن MTP او الكونفرنس وستكون DIAL PLAN بسيطة

لنتعرف الآن على الشكل الثاني من أشكال شبكات الفويس



في هذا الشكل من شبكة الفويس يكون كل شيء خاص بالشبكة من سيرفرات الكول مانجير والتطبيقات وموارد ال DSP كلها موجودة في نفس الموقع بجانب بعض وقد يكونوا في نفس الكابينة

طبعا سيسألني شخص ما هو DSP سأقول له لا تستعجل سيأتي وقته اذا وجد خط لل IP Wan قد يكون IP VPN او أي نوع من انواع توصيل الانترنت فإنه يستخدم فقط لاشارات الداتا فقط ولا يستخدم للفويس

وكما نلاحظ في الشكل هناك سحابتين واحدة خاصة بالسنترال وهي التي تتم من خلالها المكالمات ووحدة خاصة بالانترنت وتستخدم لخدمات الانترنت فقط هذا لشكل يدعم حتى 30000 جهاز تليفون لكل كالستر حيث يتكون اكبر كالستر كما درسنا من 8 كول مانجير يكون 4 شغالين و4 Backup سيقول شخص ما هو الكالستر (Cluster)

الاجابة :

سأقتبس حرفيا من كلام استاذنا ايهاب وليسامحني لنقل اجابته حرفيا ولكنها اجابة كافية واكثر من رائعة ولا داعي للزيادة عليها

وطبعا هذا يوفر المجال في حالة استخدام IP WAN لان سعة خط IP WAN ليست كالسعة المتاحة لي داخل الشبكة

هذا في حالة الصوت فمما هو الوضع في حالة استخدام الفيديو في الموقع الواحد نستخدم 384 HIGH BANDWIDTH VIDEO كيلو بت او اعلى وفي حالة الاتصال بموقع بعيد عن طريق ال IP WAN فلن نستطيع استخدام هذا البانديت لان سعة كل موارد الشبكة ولذلك نستخدم LOW BANDWIDTH VIDEO من 128 كيلو بت او اقل

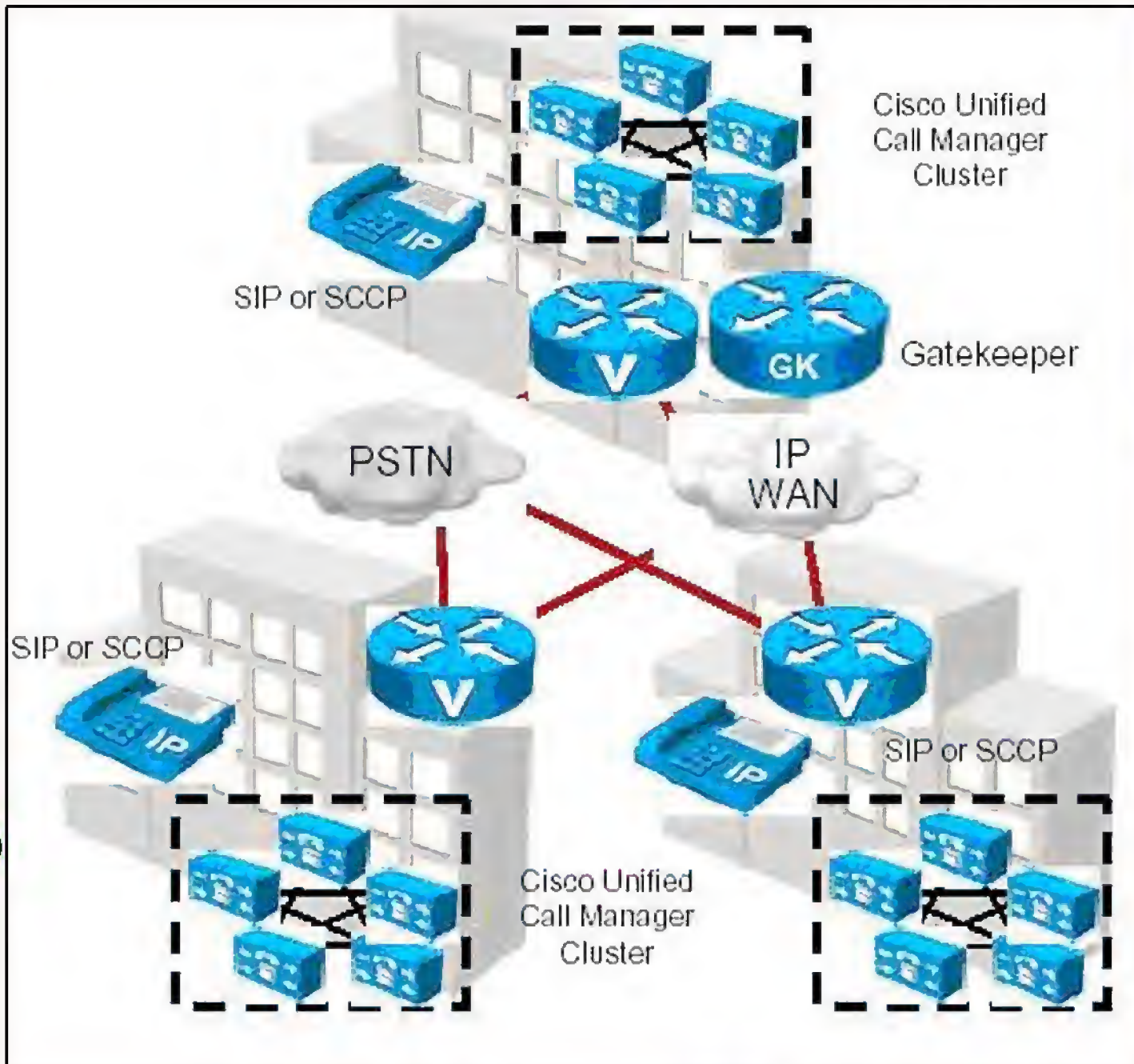
نقل الفيديو عبر الشبكة غير مفضل على السرعات 768 كيلو بت أو أقل ولذلك فإن CISCO UNIFIED VIDEO ADVANTEGE WIDEBAND CODEC الذي يعمل على سرعة 7 ميغا لا يستخدم الا داخل الموقع الواحد فقط

- ال CAC و AAA و SRST الاصدار الرابع وما بعد يدعم الفيديو
- الاصدار قبل الرابع من SRST لا يدعم الفيديو

للمحافظة على الشبكة في حالة وقوعها نستخدم
★ في حالة SCCP PHONES نستخدم SRST على الفويس جيت واي CISCO UNIFIED VOICE GATE WAY ROUTER او على CISCO UNIFIED COMMUNICATIONS MANAGER EXPRESS يعمل في حالة SRST

★ في حالة SIP PHONES نستخدم SIP SRST
★ في حالة MGCP PHONES نستخدم MGCP GATEWAY FALLBACK

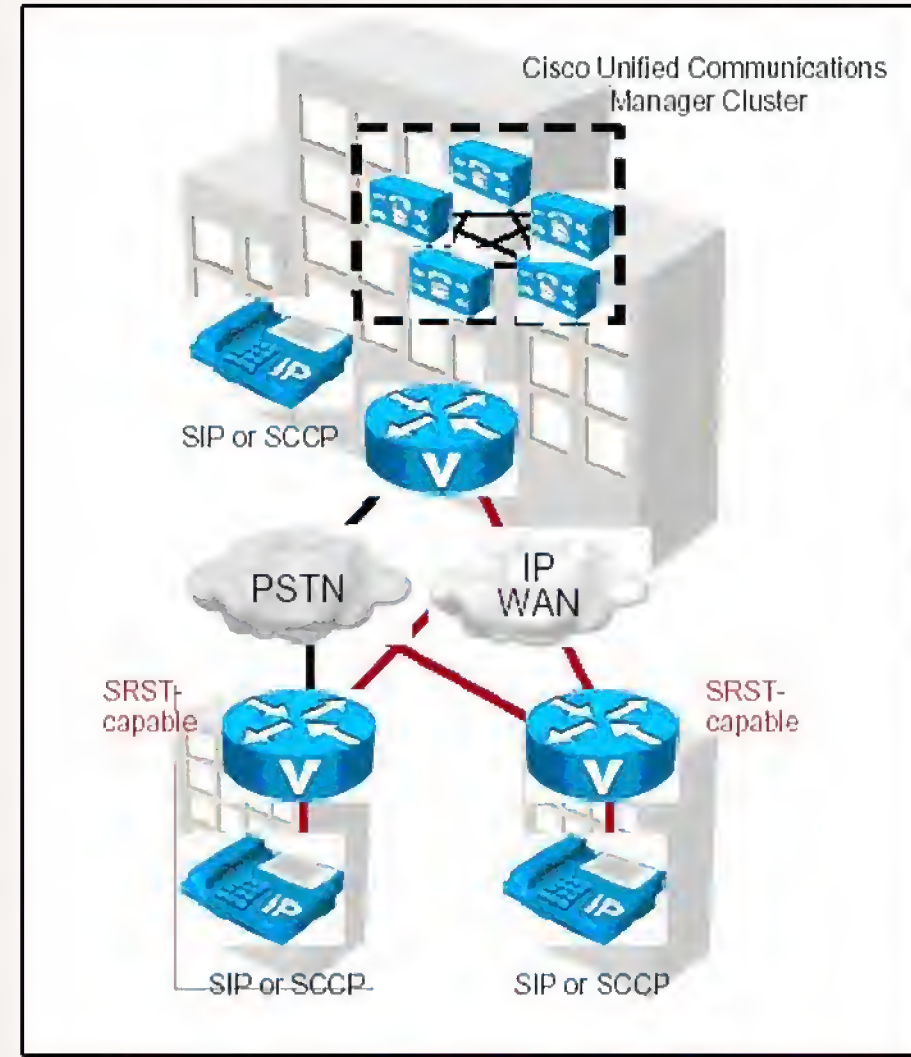
★ يفضل استخدام HSRP للمحافظة على الرواترات ووجود احتياطي دائما في حالة وقع الرواتر الرئيسي
مواقع متعددة مع مراكز تحكم متعددة Multisite WAN with Distributed



في هذا الشكل نرى ان كل موقع يحتوي على الاجهزة الخاصة به ولا يحتاج الى المواقع الاخرى من اجل اتمام عملية الاتصال يدعم حتى 30000 تليفون sccp او SIP او جهاز فيديو يدعم حتى MGCP gateway 1100 او H.323 كما في النظام السابق الكودك High codec يكون بين نفس الموقع وال low codec يكون بين المواقع البعيدة عن بعضها لتوفير البانديت عبر الشبكة نستخدم CAC وال AAA من من مزايا هذا التصميم ان الشبكة لن تتأثر عند سقوط خط IP WAN يدعم هذا الشكل مئات المواقع

الى اللقاء في موضوع بسيط اخر لتبسيط مفاهيم الشبكات للمبتدئين

Multisite WAN with Centralized Call Processing



في هذا الشكل يكون هناك اي عدد من المواقع غير محدد ولكن هناك موقع واحد فقط هو الذي يوجد به الكول مانجير الذي يتحكم في الكل هذا الشكل يختلف عن الشكل الاول المفرد في ان المكالمات للمواقع البعيدة تحمل من خلال IP WAN لكن ماذا سيحدث لل IP WAN ان تحولت الى DOWN هل ستقع الشبكة؟؟؟ بالطبع لا

الذي سيحدث أننا سننتقل الى SRST وهي SRST Survivable Remote Site Telephony وهي خاصية تجعل الراوتر هو الذي يعمل بدلا من الكول مانجير أي أنه سيعمل يقوم بعمل ال call processing وبذلك التليفون لن يشعر بغياب شيء وستستمر الشبكة في العمل في الشبكات المتعددة يتم استخدام ال CAC وهو Call Admission Control وهو ضروري جدا للحفاظ على الشبكة حيث انه يحدد البانديت ويوزع ال BANDWIDTH لكل كالستر او بمعنى اخر سيحدد عدد المكالمات المسموح لكل كالستر واذا زاد عدد المكالمات عن العدد المسموح سيتم تحويل المكالمات للمرور عبر PSTN (السنترال) .

طب هل اذا زاد عدد المكالمات عن العدد المسموح سيتم استخدام خطوط السنترال تلقائيا
الاجابة: لا هناك AAA وهو اختصار ل automated alternate routing وكما هو واضح من الاسم فهو لاختيار المسار البديل عن سقوط المسار الاول وطبعا لن يكون العدد كبيرا كما في حالة استخدام الكول مانجير فكل راوتر يدعم عدد معين من التليفونات على حسب موديل الراوتر ملحوظة مهمة جدا

يجب وضع QOS على الرواترات لاننا في هذا الشكل نستخدم الفويس عبر IP WAN وفي هذه الحالة لا بد من توضيح الأولوية للراوتر لكي يمرر مكالمات الصوت قبل الداتا فليس من المنطقي ان ارسل ايميل ويتم وصوله في نفس اللحظة وعندما اتكلم مكالمة صوتية انتظر عشر دقائق لوصول كلمة الو وهذا الشكل يدعم حتى 30000 تليفون لكل كالستر ولكن DSP هنا سنستخدمه لعمل transcoding

★ العدد الاقصى للمواقع 1000

★ عدد H323 هو 1100 مثل السابق

★ الكودك المستخدم بين الموقع الواحد يكون HIGH BANDWIDTH مثل G722, G711

★ الكودك المستخدم بين المواقع البعيدة يكون LOW BANDWIDTH مثل G729 H, G28

★ طبعا هنا البعض سيقول ما الفرق بين هذا وهذا
الاجابة

في حالة استخدام الكودك الاعلى ل 711 فإننا سنستخدم BANDWIDTH اعلى (64 كيلو) طبعا هذا رقم صغير في حالة استخدامه داخل اللان لأن اقل مجال في الشبكة المحلية سيكون 100 ميغا او اكثر اما LOW BANDWIDTH CODEC فهو كودك يتم ضغطه من 64 كيلو الى 8 كيلو

خمس أشياء يجب أن تعرفها عن سويتشات سيسكو

الشيء الرابع : التحكم في سرعة المنفذ وال Duplex ؟

يعد موضوع التحكم في سرعة المنفذ وأعداد ال Duplex من أكثر الأشياء التي قد تؤدي إلى حدوث مشاكل في هذا النوع من الأجهزة بسبب وجود تعارض بين أعدادات المنفذ الموجودة على السويتش وأعدادات المنفذ الخاص بجهاز الكمبيوتر المتصل معه لهذا نستخدم الأمر `show interface` متبوعاً بنوع ورقم المنفذ من أجل التأكد من مطابقة الأثنان مع بعضهما البعض وهذا مثال يوضح كيف سوف تظهر النتائج

```
Switch#show interfaces fastEthernet 0/1
FastEthernet0/1 is down, line protocol is down (disabled)
Hardware is Lance, address is 0005.5e2d.3e01 (bia 0005.5e2d.3e01)
BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
```

ويتضح لنا أن سرعة المنفذ هي 100 وان حالة ال Duplex هي Full ولو في حال اردنا تغيير هذه الأعدادات مثل تغيير سرعة منفذ واحد غيغاً إلى 100 وتغيير حالة ال Duplex إلى half نقوم بتنفيذ الأوامر التالية

```
Switch(config)# interface gigabitEthernet 1/0
Switch(config-if)# speed 100
Switch(config-if)# duplex half
```

الشيء الخامس : كيف أزيد من الأمن والحماية للمنافذ المستخدمة ؟

تدعم أغلب أجهزة سيسكو خاصية جميلة وهامة تدعى ال Port Security وهي تسمح لنا بالتحكم في عدد الأجهزة التي يجب أن تعبر من خلال هذا المنفذ (في حال لو كان هذا المنفذ مرتبط مع هوب مثلاً) بالإضافة إلى أنها تسمح لنا بتحديد رقم الماك أدريس الذي يملك الصلاحية في العبور ولأعدادها يجب أن نتوجه إلى كل بورت ونقوم بتنفيذ الأعدادات التالية

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```

بتفصيلنا لهذه الخاصية نخر السويتش بأن عدد الأجهزة المتاحة للعبور هي واحد فقط وهو أول ماك أدريس يعبر من خلال هذا المنفذ وهذا طبعا يساهم في حماية السويتش والشبكة من الأختراق أو التجسس .



في أغلب الأحيان تكون استخدامتنا للسويتش على مستوى بسيط في البيت أو شركة صغيرة أو مدرسة الخ... وعادة تكون هذه السويتشات من نوع plug and play يعني نقوم بتوصيل الأجهزة وأنتهى عمل السويتش بحيث لا يمكننا أعداد أو تغيير أي شيء على السويتش ولاحتي إصلاح الأعطال أن وجدت ومن هنا قد يفكر أحدنا بشراء سويتشات أفضل من حيث الأداء والتحكم مثل سويتشات سيسكو والتي سوف أخصها بهذا المقال ولنفرض ان خبرتك مع التعامل مع هذا النوع من الاجهزة بسيطة جدا لذا أحببت أن أطرح في هذا المقال الأشياء الخمسة التي يجب أن تعرفها حول هذا النوع من أجهزة سيسكو بغض النظر عن خبرتك في التعامل معها

الشيء الأول : ماهو ال Vlan وماهو ال Default Vlan ؟

ال Vlan أو Virtual Lan هي خاصية تسمح لنا بعزل المنافذ عن بعضها البعض على شكل مجموعات والتي تعطي للشبكة شيئا مهماً الأول هو الأداء الأفضل للشبكة فمن خلال عزل هذه البورتات عن بعضها سوف نقوم أيضا بعزل ال Broadcast أيضا عن المنافذ بحيث لو خرج broadcast من أحد مجموعات ال Vlan فسوف يقتصر فقط على هذه المجموعة ولن ينتشر على كل المنافذ والشيء الثاني وهو الأمن والسيكورتى فهي تتيح لنا عزل الأشخاص تماما عن بعضهم وبالتالي هذا يؤمن سرية وحماية أكبر للمستخدمين الموجودين على الشبكة أما ال Default Vlan فهي عادة Vlan1 وهي عادة تضم كل المنافذ الموجودة على السويتش ونستطيع مشاهدتها من خلال كتابة الأمر Show vlan كما في الشكل التالي

Switch#show vlan		
VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2

الشيء الثاني : لماذا أعطي السويتش أيبي ؟

كما هو معروف عن السويتشات الخاصة بالطبقة الثانية ال data link بأن تعاملها مع الترافيك يتم من خلال الماك أدريس فقط لكن مع سويتشات سيسكو هناك إمكانية إعطاء السويتش أيبي لهدف واحد فقط وهو من أجل إتاحة التحكم بالسويتش عن بعد مثل استخدام التلنت أو ال SSH أو من أجل مراقبة عمل وأداء السويتش وهي تتم من خلال إعطاء ال Vlan أيبي ومن خلال الأوامر التالية

```
Switch(config)# interface vlan1
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
```

الشيء الثالث : كيف أجعل البورتات تعمل بشكل أسرع ؟

تقوم سويتشات سيسكو بعدة أمور وأشياء قبل تفعيل المنفذ لكي يعمل وهي عادة تكون من أجل التأكد من عدم وجود loop في الشبكة لهذا نلجأ إلى عمل بعض الأعدادات لكي يقوم السويتش مباشرة بتفعيل المنفذ وهذه الأعدادات يجب أن تكون على البورتات المتصلة مع أجهزة كمبيوتر أو سيرفرات وهي كالتالي

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# no shutdown
Switch(config-if)# spanning-tree portfast
```


كيف تفهم اجهزة الطبقة الثانية ترافيك الـ Multicast ؟

بقلم: أيمن النعيمي

من خلال هذه الصورة سوف نلاحظ النقاط التالية

★ أن أول Octet من الأيبي لا يضاف في عملية التحويل من الأيبي ملتي كاست إلى الماك أدريس ملتي كاست وهذا يقودنا إلى حقيقة أن التحويل يتم من خلال التعامل مع

الثلاث أجزاء الأخيرة من الأيبي

★ أول 24 بت دائما 01-00-5e

★ البتات المتاحة لعملية التحويل هي 23 بت فقط

★ ان البت الخامس والعشرين هو دائما صفر وهذا يقودنا إلى شيء مهم جدا وهو

حدوث Over looping في عملية التحويل مما يعطي لكل 32 آيبي ملتي كاست

نفس عنوان الماك لناخذ مثلا واقعيًا لعملية التحويل ولكن 229.239.80.1 أو

خطوة سوف نقوم بها هي تحويل هذا الأيبي إلى Binary وسوف يكون بالشكل التالي

11100010.11101111.01010000.00000001

الرقم إلى لغة الـ HEX لكن لتتوقف قليلا قبل بدأ التحويل ونأخذ النقاط السابقة

أول شيء يجب علينا أن نفعله هو كتابة الرقم الذي وضعته الأيانا وهو 01-00-5e

وبعدها سوف نأخذ آخر 23 بت من الأيبي ونضيف لها زيرو التي تمثل البت 25

لتكون الصيغة كالآتي 01101111.01010000.00000001

هذه الأرقام إلى لغة الـ HEX لتحصل بعدها على النتيجة التالية 6f-60-01

ونضيفها إلى القسم الأول من الماك أدريس لنحصل على الصيغة الكاملة للماك أدريس

ملتي كاست وهو 01-00-5e-6f-60-01 لناخذ مثال آخر وهو الأيبي 231.111.

80.1 ونقوم مباشرة بتحويلها إلى binary لنحصل على 11100111.

01101111.01010000.00000001 بعد استثناء أول octet منها أي أول

ثمانية بت وآخذ آخر 23 بت سوف نحصل على 01101111.01010000.00000001

برائيك ماذا سوف تكون النتيجة ؟ طبعا سوف تكون

نفس النتيجة السابقة وهي 01-00-5e-6f-01 ولو كررنا هذه العملية مع تغيير

أول ثمانية بت ومع استخدام نفس الرقمان الذي وضعتهما في المثال السابق وهما

138,111 سوف نحصل على 32 حالة تكرار لذا هذه النقطة هي أهم نقطة لدينا

اليوم وهو عدم إنشاء مجموعتان ملتي كاست في شبكة واحدة من دون مراعاة هذا

الموضوع وهذا مثال آخر يوضح كل الأيبيات التي تتكرر في الماك أدريس ملتي كاست

224	1	1	1
224	129	1	1
225	1	1	1
225	129	1	1
226	1	1	1
226	129	1	1
227	1	1	1
227	129	1	1
228	1	1	1
228	129	1	1
229	1	1	1
229	129	1	1
230	1	1	1
230	129	1	1
231	1	1	1
231	129	1	1
232	1	1	1
232	129	1	1
233	1	1	1
233	129	1	1
234	1	1	1
234	129	1	1
235	1	1	1
235	129	1	1
236	1	1	1
236	129	1	1
237	1	1	1
237	129	1	1
238	1	1	1
238	129	1	1
239	1	1	1
239	129	1	1

32 Multicast IP addresses
Encoding to the same
Multicast MAC

bits not
encoded

00000001	00000000	10111110	0	00000001	00000001	00000001
01	00	5E	01	01	01	01

دائما ماسمعنا عن الـ Multicast وعرفنا أنه عبارة عن طريقة ينتقل فيها

الترافيك على مجموعة معينة من الأشخاص على الشبكة وعرفنا أيضا بأن له رانج

خاص من الأيبي يبدأ من 224.0.0.0 وينتهي بي 239.255.255.255

ولكن السؤال الآن كيف يتم التعرف على الـ Multicast Traffic على مستوى

الطبقة الثانية وكيف يتم حسابها ؟

بداية يجب أن نعلم ان الماك أدريس يتألف من 48 بت وهي مقسمة إلى قسمين أول

قسم والذي يشكل أول 24 بت خاصة بي الـ OUI او خاص بالشركة المصنعة

لكرت الشبكة وهي ثابتة للشركة وثاني 24 بت تملك الشركة الصلاحيات الكاملة

لتغييرها بحيث تعطى لكل كرت شبكة رقم خاص يختلف عن باقي الأرقام ومن

هنا أحب أن أدخل في الموضوع فلكي تفهم الأجهزة التي تعمل على الطبقة الثانية

الترافيك الخاص بي الـ Multicast كان لابد من توفير عنوان فيزيائي يعبر

عن الـ Multicast ومن هنا قامت منظمة الأيانا بتوفير عنوان OUI خاص

بي الملتي كاست وهو 01-00-5e وهذا يعني ان لدينا 24 بت يجب ان تكون

للأيبي لكن لتتوقف قليلا ونفكر في هذه المشكلة الكبيرة فكلنا يعلم أن الأيبي يتألف

من 32 بي ومالدينا هو 24 بت يعني هناك 8 بت لا يوجد لها مكان في الماك أدريس

ولكي تكبر المشكلة أكبر الأيانا قالت لك أن البت 25 دائما صفر وهذا يزيد العدد إلى

9 بت إذا ما هو الحل ؟

أولا جميعنا يعلم أن الكلاس D يبدأ دائما بي 1110 يعني كل الأيبيات الخاصة

بالميلتي كاست لها نفس الأربعة بت الأولى ونستنتج من هذا الكلام أن كتابة أول اربع

بت لا يوجد لها أي داعي لذا عدد البتات سوف ينقص بمقدار اربعة وسوف يكون

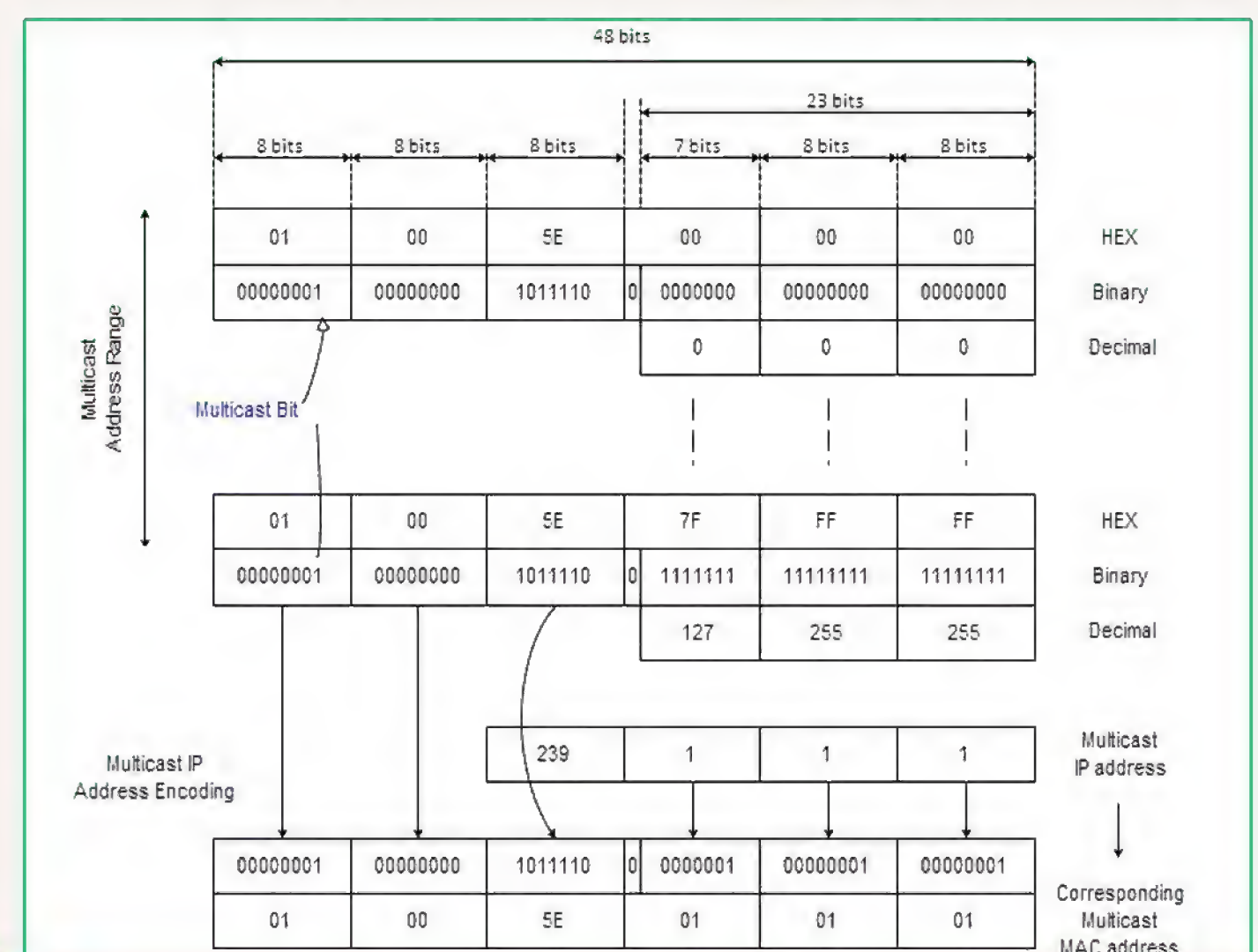
الباقى هو 5 بت مازالت تشكل بالنسبة لنا مشكلة وهذا جدول توضح الفكرة

الأولى من الحل

IP Multicast	IP Multicast (binary)
224.0.0.0	11100000.00000000.00000000.00000000
225.0.0.0	11100000.00000000.00000000.00000000
227.0.0.0	11100011.00000000.00000000.00000000
230.0.0.0	11100110.00000000.00000000.00000000
237.0.0.0	11101101.00000000.00000000.00000000

لناخذ الصورة التالية ونبدأ الحديث بشكل أعمق وهي توضح في القسم الأول منها

الأيبي 224.0.0.0 والقسم الثاني 239.255.255.255 والثالث 239.1.1.1



قسم أمن وهماية الشبكات

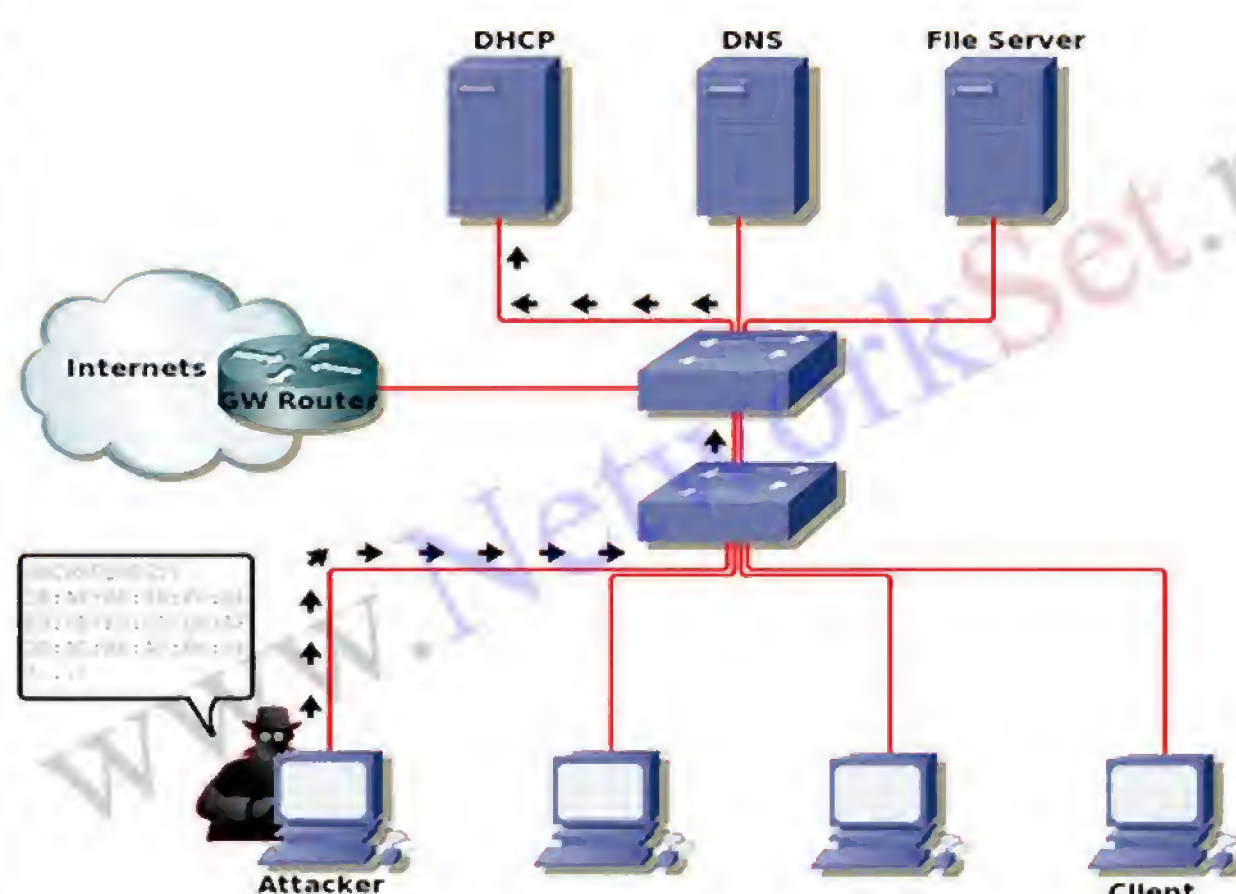
هذا القسم سوف يتم عرض فيه كل الأمور الواجب عملها في الشبكة بهدف التخفيف من نسبة القرصنة التي تحدث على الشبكة وأرجو منك أن تدقق على كلمة تخفيف لان النظرية العامة تقول لا يوجد جهاز آمن خالي من الثغرات مهم كانت قوته!



هجوم الـ DHCP Starvation وطريقة التصدي له

ماهو DHCP ؟

الـ DHCP أو Dynamic Host Configuration Protocol وهو أحد البروتوكولات الموجودة في أغلب الشبكات والسيرفرات ووظيفته الرئيسية هي إعطاء الأجهزة الموجودة على الشبكة أيا كان نوعها روترات سيرفرات أجهزة كمبيوتر المعلومات اللازمة للاتصال مع الشبكة وهذا يشمل الأيبي والماسك والجيت واي والـ DNS Server لذا فهو يشكل عصب الشبكة وتعطيله أو قرصنته قد يسبب لك مشاكل قد لاتنتهي لذا سوف نستعرض في هذا المقال أحد الهجمات التي تؤدي إلى تخريب عمل السيرفر وتعطيله



ماهو هجوم DHCP Starvation ؟

يشكل هذا النوع من الهجوم خطرا كبيرا على الشبكة لانه يقوم ببساطة بحجز كل الأيبيات الموجودة في سيرفر الـ DHCP وفيها يقوم المهاجم بأرسال عدد غير محدود من الرسائل إلى سيرفر الـ DHCP يطلب فيها تزويده بأيبي للجهاز الخاص فيه وعندما يتم أستلام الأعدادات من السيرفر وحجز الأيبي له يقوم بأرسال طلب جديد إلى السيرفر لكن هذه المرة بماك أدريس مختلف وهكذا حتى يقوم المهاجم بحجز كل الأيبيات المتاحة على السيرفر وحتى لو كانت 10000 أيبي لان هذه العملية تتم بسرعة كبيرة والتي قد لاتستغرق بضع دقائق وبالتالي أي محاولة من أي جهاز آخر موجود على الشبكة للحصول على أيبي من السيرفر سوف تباء بالفشل

طريق الحماية من هذا النوع من الهجوم

طريقة الحماية تم التطرق لها من قبل وهي تتم من خلال البورت سكيورتي وذلك بتحديد عدد معين من الماك ادريس المسموح لها بالدخول من خلال هذا المنفذ والأوامر طبعا سوف تطبق على السويتش بالشكل التالي

Cisco's CAT IOS

```
set port security 1/2 enable
set port security 1/2 port max 1
set port security 1/2 violation restrict
set port security 1/2 age 500
```

أما أعدداده على أجهزة جونيبر فهو يتم من خلال الأوامر التالية :

Juniper's JUNOS

```
set interface ge-0/0/1 mac-limit 1
set interface ge-0/0/1 allowed-mac 00:11:22:33:44:55
```

الأمر الأول لتحديد عدد العنوين الفيزيائية المسموح له بالاتصال والأمر الثاني من أجل تحديد عنوان الماك ادريس الذي يملك الصلاحية للاتصال مع هذا المنفذ كلمة أخيرة هذا النوع من الهجوم قد لا يكون الهدف منها حجز كل الأيبيات الموجودة على الشبكة لان المهاجم قد يكون هدفه من نوع آخر وهو القيام بي الـ DHCP Spoofing وهو موضوعنا للعدد القادم إن شاء الله

Cisco's IOS

```
Switch# conf t
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```


Radius Server

Remote Authentication Dial in User Service

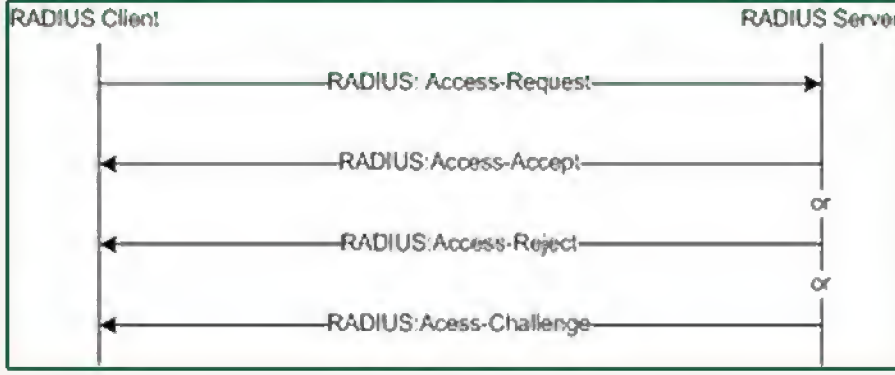
بقلم أحمد بخيت

في العالم الحقيقي والعملي نجد أن البورتات المستخدمة هي:

البورت 1645 يتم استخدامه في Radius Authentication

البورت 1646 يتم استخدامه في Radius Accounting

لذلك فإن العديد من السيرفرات تقوم أولاً بعمل استكشاف للبورتات المستخدمة من الطرف الثاني حتى تتكيف معها، مع العلم أن كلا من سيسكو وجونيبر تتعامل مع البورتات الأخيرة.



في هذا الشكل لدينا عميل Radius Client يقوم بطلب وصول من ال Radius Server وهنا لدينا ثلاثة سيناريوهات

محتملة وهي أن يقبل السيرفر هذا الطلب ويقوم بإرسال رسالة Radius Access Accept أو أن يتم رفض هذا الاتصال من خلال Reject أما الحالة الأخيرة هي زيادة في التأكيد مثل طلب معلومات أكثر من العميل مثل PIN Code وما إلى ذلك.

وبالنظر إلى الجانب الأمني لدى هذا السيرفر فإنه في الحالة الطبيعية يقوم بإرسال بيانات تأكيد الدخول في الصورة PAP أي في صورة غير مشفرة ولكنه متاح لدى أي مدير شبكة بأن يقوم بعمل شيء من التعديلات على ذلك ويرسل هذه المعلومات في صورة مشفرة ويقوم باستخدام تقنيات أخرى مثل MD5, Chap وهذا شيء من القوة لكن الأكبر هو عمل الاتصال من البداية بصورة آمنة مثل استخدام تقنيات قوية كما يحدث في IPsec.

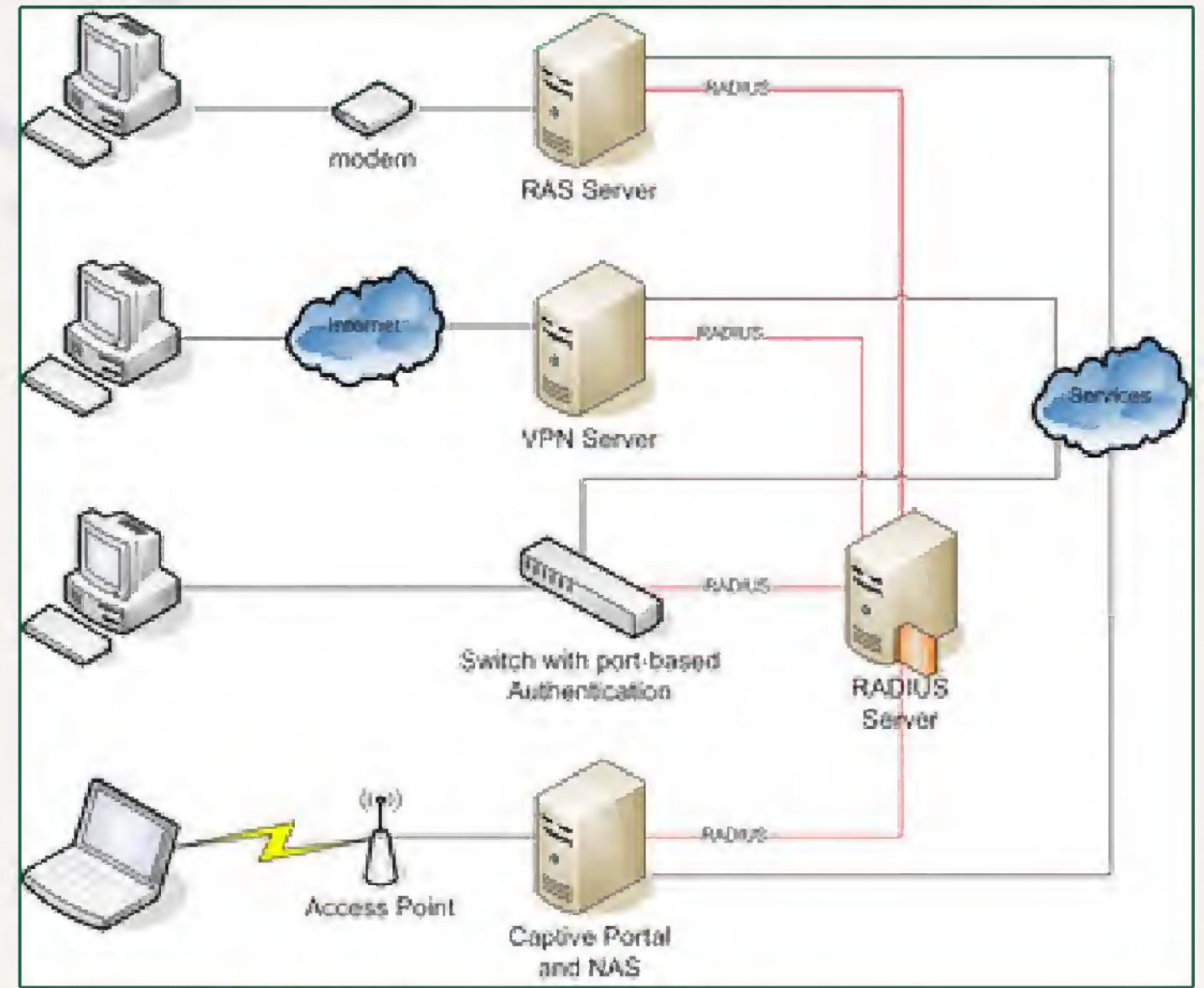
نأتي لقسم خاص يتحدث عن تجربة شخصية قد واجهتني مرات ومرات، حيث أنه في بداية المقال قد ذكرنا أن استخدام مثل هذا البروتوكول يكون مع الشبكات الكبرى أو شبكات مزودي الخدمة، لكن وعن تجربة شخصية أجد أن أغلب مديري الشبكات ممن لديهم توقع بأن شبكاتهم الصغيرة ستكون وتصير شبكات كبيرة نجدهم قد يلجئون إلى هذا البروتوكول من البداية عند التصميم حتى لو كانت شبكاتهم صغيرة الحجم لأنهم يطلبون الناحية التنظيمية وشئ من المركزية خاصة في شأن معلومات الدخول على البنية التحتية Infra-Structure لشبكاتهم وكذلك لو كانت هذه الشبكات ذات تقنيات متطورة في الربط مثل استخدام ال MPLS حيث الشبكات الدولية - كما أحب أن أسميها - لذلك نجد دخول تقنيات أمنية في تشفير هذا الاتصال وحمايته بشتى الطرق.

ومن هنا وهناك نجد أن لهذا البروتوكول اسم آخر قد استخدمناه في هذا المقال وهو السيرفر، وهذا مقصود إذ أن أغلب تطبيقاته قد تمت على سيرفرات لينكس المتميزة بالقوة والثبات في الأداء، حيث قصة نجاح قد بدأت منذ عام 1990 واستمرت إلى يومنا هذا وستستمر إلى ما شاء الله.

هو بروتوكول هام و واسع الطلب في الشبكات حيث يتم استخدامه في عمل شئ من المركزية لكل من ثلاث وظائف رئيسية وهي Authentication, Accounting, Authorization حيث يطلق عليها AAA حيث إدارة الحواسيب لتكون قادرة على الاتصال بالشبكة من خلال هذه الخدمة، ومن أهم التطبيقات لهذا السيرفر هو ما يسمى بال Access Server ، وقد تم ابتكاره عام 1991 على يد شركة Livingston Enterprises, Inc.

ويغلب على هذا البروتوكول الاستخدام الضخم حيث يقبل عليه مزودي الخدمة والشركات ذات الحجم الكبير حيث أنه يوفر لهم وسيلة آمنة ومركزية في عمل تأكيد لعمليات الدخول على الانترنت والشبكات الداخلية للشركات والشبكات اللاسلكية وكذلك خدمات الایمیل مهما كانت وسيلة الاتصال بهذه الخدمات سواء كانت مودم أو نقاط وصول أو VPN أو غيرها.

يعمل هذا البروتوكول في صورة Client/Server إذ أنه لابد من توافر كلا طرفي الاتصال حتى تعمل الخدمة فلا يمكن عدم تواجد السيرفر إذ أن الاتصال أو عملية تأكيد الدخول لا يمكن تأكيدها منه، ويعمل هذا البروتوكول على ال Application Layer مع استخدام الاتصال من النوع UDP في الانتقال من السيرفر نفسه إلى العميل ومن المتوقع لدى الجميع وليس المفاجئ أن هذا البروتوكول يعمل بالأساس على سيرفرات لينكس بصورة كبيرة مع سيرفرات ويندوز NT مع العلم أنه كلما زادت عمليات تأكيد الدخول كلما كان اللجوء إلى النظام لينكس اكبر واكبر لما يتميز به هذا النظام من استقرار.



وهنا توجد ملحوظة هامة أظن أنه لابد من توضيحها لدى العديد إذ أن هذا البروتوكول لا يتم استخدامه فقط مع المستخدم في الصورة البشرية فقط، لكنه يتم التعامل به بين الأجهزة فيما بينها إذ أنه في تكنولوجيا ADSL كمثال فإنه يتم ربط أجهزة ال DSLAMs وهي المسؤولة عن إيصال خدمة الانترنت لدى العميل النهائي فإن هذه الأجهزة تتصل مع مثيلاتها التي تسبقها في هيكل شبكة مزود الخدمة باستخدام هذا البروتوكول، وكذلك مع أجهزة الراوتر لدى العميل وأجهزة ال DSLAM تتم باستخدام هذا البروتوكول، لذلك تصوروا معي مدى الاعتماد على هذا البروتوكول في الجانب العملي.

هذا البروتوكول يتعامل مع بورتات عديدة وهي :

البورت 1812 يتم استخدامه في Radius Authentication

البورت 1813 يتم استخدامه في Radius Accounting

مع العلم أن هذه البورتات لا توجد إلى عند مؤسسة ال IANA فقط ولكن في

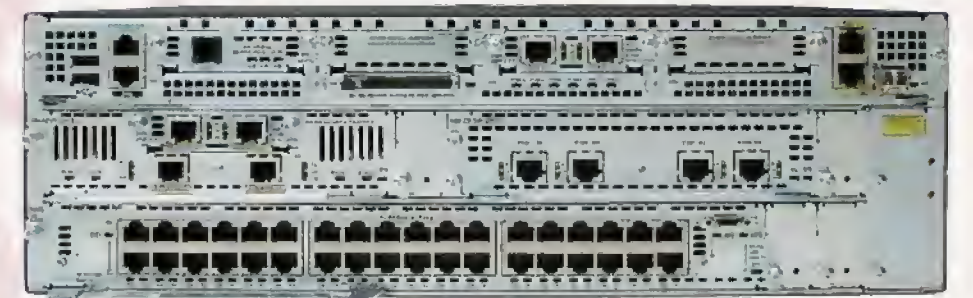
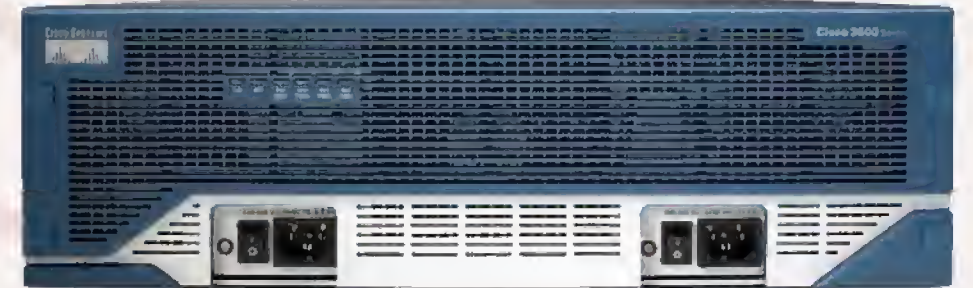
عناك و معلومات

أعداد عثمان إسماعيل

CISCO SYSTEMS



RAM	512 MB (installed) / 1 GB (max) - DDR SDRAM
Flash memory	128 MB (installed) / 512 MB (max)
Type	Router
MAX Transfer Rate	1 Gbps
Encryption Algorithm	DES, Triple DES, SSL, 128-bit AES, 192-bit AES, 256-bit AES
Supplied OS	Cisco IOS Advanced IP services
Digital Signaling Protocol	Wired
DCP	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocol Remot	SNMP 3, SSH-2
Interfaces	2 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 2 x USB 1 x management - console 1 x network - auxiliary
Firewall protection, hardware compression, hardware encryption, VPN support, MPLS support, content filtering, URL filtering, QoS, Dynamic Multipoint VPN	



CISCO 3845-HSEC/K9

RAM	128 MB
Flash memory	16 MB
Ramer Table of MAC Addr	12K entries
Authentication method	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Interfaces	management-console RJ-45 2 x network stack device
Connection Type	Half-duplex, full-duplex
Data Rate	100 Mbps
DCP	Ethernet, Fast Ethernet 10Base-T/100Base-TX
Protocol Remote	SNMP1, RMON1, RMON2, SNMP, Telnet, SNMP3
Number of Ports	48 x Ethernet 10Base-T, Ethernet 100Base-TX
Flow control, full duplex, routing, IP-routing, DHCP support, auto-negotiation, ARP support, trunking, load balancing, VLAN support, auto-uplink (auto MDI/MDI-X), IGMP snooping, manageable, IPv6 support	



Catalyst 3750 48TS-E

RAM	256 MB (installed) / 1 GB (max)
Flash memory	64 MB (installed) / 256 MB (max)
Protocol Remote	SNMP 3
Type	Voice / fax module
Interfaces	2 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 2 x USB 1 x management - console 1 x network - auxiliary
Encryption	DES, Triple DES, AES
Supplied OS	Cisco IOS SP services
OS Required	Microsoft Windows 98 Second Edition
DCP	Ethernet, Fast Ethernet, Gigabit Ethernet
Voice Codecs	G.711, G.723.1, G.728, G.729, G.729a, G.729ab, G.726



CISCO 2821-V/K9



Juniper®

NETWORKS

JUNOS Software version tested

JUNOS 10.0

Firewall performance (max)

650 Mbps

IPS performance (NSS 4.2.1)

60 Mbps

AES256+SHA-1 / 3DES+SHA-1 VPN performance

65 Mbps

SRX 100

Maximum concurrent sessions

16 K (512 MB DRAM) / 32 K (1 GB DRAM)

New sessions/second (sustained, TCP, 3-way)

2,000

Maximum security policies

384

Maximum users supported

Unrestricted

Fixed I/O ports

8 x 10/100

CX111 3G Bridge support

Yes

Firewall

- * Network attack detection: Yes
- * DoS and DDoS protection: Yes
- * TCP reassembly for fragmented packet protection: Yes
- * Brute force attack mitigation: Yes
- * SYN cookie protection: Yes
- * Zone-based IP spoofing: Yes
- * Malformed packet protection: Yes

Intrusion Prevention System

- * Stateful protocol signatures: Yes
- * Attack detection mechanisms: Stateful signatures, protocol anomaly detection (zero-day coverage), application identification
- * Attack response mechanisms: Drop connection, close connection, session packet log, session summary, email, custom session
- * Attack notification mechanisms: Structured
- Worm protection: Yes
- * Simplified installation through recommended policies: Yes
- * Trojan protection: Yes



ScreenOS version tested

ScreenOS 6.2

Firewall Perf (Large Packets)

160 Mbps

Firewall Performance (IMIX)

90 Mbps

Firewall Packets Per Second

30,000 PPS

3DES+SHA-1 VPN Perf

40 Mbps

Concurrent VPN Tunnels

25/40*

Max Concurrent Sessions

8,000/16,000*

New Sessions/Second

2,800

Max Security Policies

200

Max Security Zones

8

Max Virtual Routers

3/4*

Max Virtual LANs

10/50*

Fixed I/O

5x10/100

Mini-Physical Interface Module (Mini-PIM) Expansion Slots

2

Physical Interface Module (PIM) Expansion Slots

0

Enhanced PIM (EPIM) Expansion Slots

0

802.11 a/b/g

Optional

Convertible to JUNOS

No

Switch SSG-550M



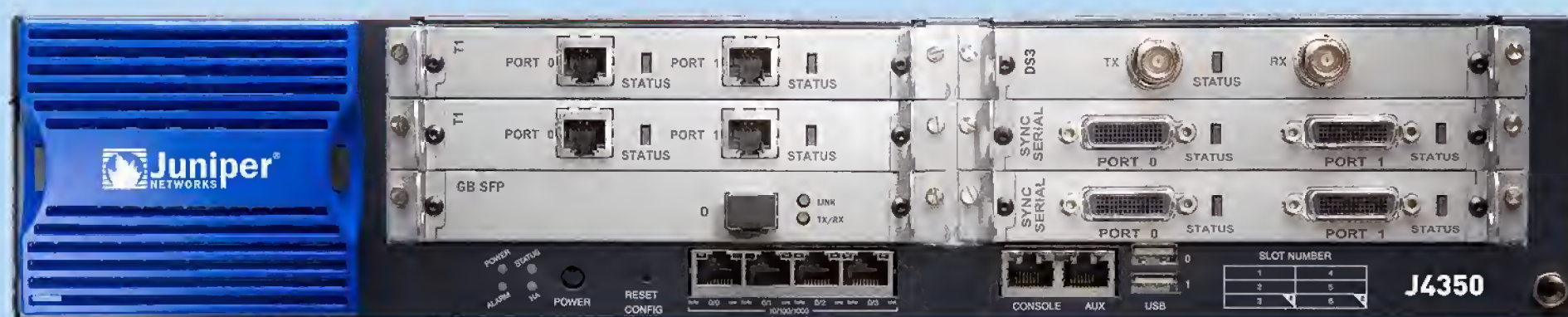
Maximum Performance and Capacity

- * Junos Software Version Support: Junos Software 9.1
- * Firewall Performance (Large Packets): 1.6G
- * Firewall Performance (IMIX): 600 Mbps
- * Firewall and Routing PPS (64 Byte): 225,000 pps
- * 3DES and SHA-1 VPN Performance: 600M
- * Concurrent VPN Tunnels: 512 MB / 1 GB DRAM 256 / 512
- * Maximum Concurrent Sessions: 512 MB / 1 GB DRAM 64 K / 128 K
- * New Sessions/Second: 10,000
- * Maximum Security Policies: 5192 (1 GB DRAM)

Network Connectivity

- * Fixed I/O: 4 x 10/100/1000
- * Maximum PIM Slots: 6
- * Maximum EPIM Slots: 2

Router J4350



Routing, Virtualization, Encapsulations

- * BGP, OSPF, RIP, Static, ECMP: Yes
- * Multicast, PIM SM, SSM, IGMP: Yes
- * Maximum Number of Security Zones: 50
- * Maximum Number of Virtual Routers: Yes
- * Maximum Number of VLANs: 512
- * PPP, FR, MLPP, MLFR, HDLC: Yes

Data Rate

- * EX3200-24P/24T: 88 Gbps
- * EX3200-48P/48T: 136 Gbps

Throughput

- * EX3200-24P/24T: 65 Mpps (wire speed)
- * EX3200-48P/48T: 101 Mpps (wire speed)

10/100/1000BASE-T Port

24 / 48 per platform

100BASE-FX / 1000BASE-X (SFP) Port Densities

4 per switch (via optional four-port GbE uplink module)

10GBASE-X Port Densities

2 per switch (via optional two-port 10GbE uplink module)

Resiliency

External redundant power supply; internal field-replaceable power supply; field-replaceable fan

Power Options

- * AC: 320W, 600W and 930W autosensing; 100-120V / 200-240V
- * DC: 190W; input voltage range 36V-72V; dual input feed

Operating System

JUNOS

QoS Queues / Port

8

Traffic Monitoring

sFlow

MAC Addresses

24,000

Jumbo Frames

9216 Bytes

IPv4 Unicast / Multicast Routes

16,000 / 8,000

Number of VLANs

4,096

Switch EX3200





مصالحات تقنية

Novell IPX : وتعني Internet Network Packet Exchange وهو أحد البروتوكولات التي تم تطويرها من خلال شركة Novel وقد تم بدا التسويق له لأول مرة عام 1980 عندما كانت الشبكات بعدها صغيرة وتعد التكنولوجيا المستخدمة في NetWare بشكل عام مأخوذة من (XNS) Xerox Network Systems وهو نظام شبكات قديم تم عمله لأول مرة عام 1970 ويملك هذا البروتوكول طبقات تختلف عن الطبقات التي عرفناها في OSI

OSI Layer : وتعني Open System Interconnection أو أنظمة الترابط المفتوحة وهو تصميم قامت به منظمة المعايير والمقاييس العالمية ISO وهو يتيح تقسيم الوظائف التي تمر بها الداتا إلى 7 طبقات مختلفة أو Layer ولكل طبقة منها هناك وظيفة أو وظائف محددة تقوم بعملها على الداتا والتي تضمن لنا اكتشاف الأخطاء وتصحيحها في كل طبقة

Physical Layer : أو الطبقة الفيزيائية وهي الطبقة الأولى من الطبقات السبعة OSI Layer وهي مسؤولة عن إرسال واستقبال المعلومات من وإلى الشبكة والقادمة من الطبقات الأعلى منها بالإضافة إلى عدة وظائف أخرى مثل تحديد الفولتات ومواصفات الكابل ومقويات Repeaters

Data Link Layer : وهي الطبقة الثانية من OSI Layer تؤمن هذه الطبقة اتصال بين الأجهزة الموجودة على نفس الشبكة مستعينة بالعنوان الفيزيائي للجهاز Mac Address ومن أهم وظائفها إيجاد أفضل وقت لإرسال الداتا والأعلام عن الأخطاء في حال حدوثها وهي تقسم إلى طبقتان فرعيتان الأولى Logical Link Control والثانية Media Access Control وهي تعد الطبقة التي يعمل عليها السويتش

Network Layer : وهي الطبقة الثالثة من OSI Layer وهي مسؤولة عن عنونة الداتا وتجهيزها بالعنوان اللازمة بالإضافة إلى إيجاد أفضل مسار يمكن الوصول إليه بين المصدر والهدف وهي الطبقة التي يعمل عليها الراوتر

Transport Layer : وهي الطبقة الرابعة من OSI Layer وهي مسؤولة عن نقل البيانات والتأكد من وصولها بشكل سليم إلى الهدف ويتم ذلك من خلال استخدام مجموعة من البروتوكولات مثل ال TCP & UDP

Session Layer : وهي الطبقة الخامسة من OSI Layer تقوم هذه الطبقة بتحديد آلية الفتح والأغلاق بين الطرفين المتصلين بالإضافة إلى إدارة الاتصال بينهم

Presentation Layer : وهي الطبقة السادسة من OSI Layer وهي مسؤولة عن أعداد البيانات من خلال ترجمتها وتنسيقها ضمن معايير متفق عليها بالإضافة إلى ضغط وتشفير البيانات أو العكس

Application Layer : وهي الطبقة الأخيرة من OSI Layer وهي طبقة البرامج والتطبيقات التي تستخدم الشبكة وهي واجهة المستخدم للاتصال مع الشبكة وتشمل هذه الطبقة برامج وتطبيقات مثل برامج تصفح الأنترنت أو البريد الإلكتروني أو برامج نقل البيانات عبر الشبكة والكثير

مشاكل وحلول

سوف يتم تخصيص هذا القسم لعرض المشاكل التي قد تواجهك في الشبكة بالإضافة إلى طريقة حل المشكلة كما أرحب أيضا بأرسال مشاكلكم على بريد المجلة magazine@networkset.net للنظر فيها وتقديم أفضل الحلول لها .

سؤال: ما أهمية الـ Process-id في الـ OSPF ؟

للإجابة على هذا السؤال يجب أن نعرف أن الـ Procsee ID في الـ OSPF لا يتعلق بباقي الروترات وهو خاص بي الروتر لوحده وبمعنى آخر local to the router only أي أن روتران في نفس الأريا سوف يعملان حتى لو كان الـ Process id مختلف وهي تفيد في حال كان الروتر يملك multiple OSPF على نفس الروتر ونريد أن تكون كل عملية منعزلة عن الأخرى لذا نلجأ لأعطاء كل عملية منها ايدي مختلف عن الآخر والرانج الخاص بها يبدأ من واحد وينتهي بي 65535 والأمر يكتب على الشكل التالي Router OSPF 3 وطبعا الأمر مختلف في EIGRP لان الـ Process id هناك يجب ان يكون موحد على كل الروترات

سؤال: ماهو local port and remote port وماهو الفرق بينهم ؟

جواب: عند دراستك للـ OSI Layer وخصوصا في الطبقة الرابعة Transport Layer سوف تجد جوابك وبشكل عام هذه الطبقة كما هو معروف عنها أنها تقوم بتحديد نوع البروتوكول المستخدم TCP أو UDP بالإضافة إلى وظائف أخرى وطريقة الاختيار ترجع إلى نوعية التطبيق الذي تستخدمه فإذا كنت تستخدم تطبيق الـ HTTP وتريد ان تتصفح أحد المواقع فأنت تستخدم أحد البورتات العشوائية الموجودة عندك للاتصال مع البورت 80 وكما هو معروف ان عدد البورتات هو 65536 أول 1023 بورت محجوز لخدمات معينة مثل http,ftp,dns,dhcp الخ وباقي البورتات تعتبر للاستخدام العام فمنها من يستخدم لبعض البرامج مثل الماسنجرات أو اي برنامج يتطلب استخدامه الأنترنت لذا الفكرة ببساطة هي ان الـ local Port هو الـ Source Port الذي يتم كتابته في الهيدر الخاص بي الـ TCP او الـ UDP بينما الـ Remote Port هو الـ Destination Port فعندما تتصفح الأنترنت أو اردت طلب صفحة معينة فأنت تضع في الهيدر الخاص بي الـ TCP رقم بورت عشوائي وليكن 1025 وهو يمثل السورس بورت أو لوكال بورت بينما تضع البورت 80 ليكون هو الـ ريموت بورت أو الـ Destination Port والسبب يعود كون التطبيق الخاص بي الـ HTTP في السيرفر الي يحوي الموقع يكون مفتوح على البورت 80 ويتسمع على انواع الترافيك الذي يصل اليه وعندما يصل الطلب سوف ينظر الى الهيدر ليكتشف أن هذا الطلب قادم لخدمة الـ HTTP فيأخذ الطلب ويضع المطلوب بداخله ويعيد ارساله لكن هذا المرة سوف يرد بان يضع اللوكال بورت رقم عشوائي بينما الـ ريموت بورت سوف يكون 80

مشكلة: انا عندي فى الشغل روتر سيسكو 1841 وأريد أن طريقة أقوم بوصل الأنترنت مع الروتر من خلال مودم DSL فماهي الإعدادات اللازمة للقيام بهذا الموضوع ؟

الحل: كل ما عليك ان تقوم به على الروتر هو default route للشبكة من خلال الأمر 192.168.1.1 0.0.0.0 0.0.0.0 ip route 0.0.0.0 0.0.0.0 172.16.1.1 ip default-gateway ويكون أيبي المودم وبعدها أتجه إلى السويتش وقم بكتابة الأمر التالي 172.16.1.1 ip default-gateway ويكون أيبي طبعاً خاص بالمنفذ الموجود على الروتر والمتصل مع السويتش (الخطوة الثانية تقوم بعملها في حال كان السويتش عندك قابل للأعداد) ملاحظة صغيرة تقنية الـ PAT مفعلة على الروتر By Default